МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению лабораторных работ
по дисциплине
«КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»
для студентов
Специальности 10.05.03 Информационная безопасность автоматизированных систем
Специализация «Анализ безопасности информационных систем»

Ставрополь
2026

Оглавление

ВВЕДЕНИЕ

Цель и задачи освоения дисциплины

Целью освоения дисциплины «Комплексное обеспечение информационной безопасности автоматизированных систем» является формирование у будущего специалиста по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация «Анализ безопасности информационных систем» системных знаний, умений и навыков по обеспечению защиты информации в автоматизированных системах с использованием комплексного подхода, включающего программно-аппаратные, криптографические, технические и организационно-правовые методы и средства. В результате освоения дисциплины студенты должны уметь анализировать угрозы, разрабатывать и внедрять эффективные меры защиты информации, обеспечивать безопасность автоматизированных систем при их эксплуатации, а также управлять рисками и реагировать на инциденты информационной безопасности в условиях современных киберугроз.

Лабораторная работа 1.
Изучение содержания и последовательности работ по защите информации
Цель работы: изучить содержание и последовательность работ выполняемых при построении комплексной системы защиты информации. Закрепить знания полученные на лекции.

Теоретическая часть
При создании комплексной системы защиты конфиденциальной информации необходимо защищать информацию во всех фазах ее существования - документальной (бумажные документы, микрофильмы и т.п.), электронной, содержащейся и обрабатываемой в информационных системах и отдельных средствах вычислительной техники, включая персонал, который ее обрабатывает - всю информационную инфраструктуру. При этом защищать информацию необходимо не только от несанкционированного доступа к ней, но и от неправомерного вмешательства в процесс ее обработки, хранения и передачи на всех фазах, нарушения работоспособности информационной системы, воздействия на персонал и т.п.

Целью работы должно являться построение комплексной системы защиты конфиденциальной информации (далее по тексту КСЗИ). Это предполагает необходимость использования, создания и разработки совокупности организационных и технических элементов КСЗИ, взаимообусловленных и взаимоувязанных, и базируется на использовании методологии построения комплексной системы защиты конфиденциальной информации.

Методология есть совокупность способов и приемов рассмотрения вопросов информационной безопасности и методов их решения в целях построения комплексной системы информационной безопасности. Она дает возможность в рамках единого подхода использовать согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Организационные и технические меры защиты информации, реализуемые в рамках КСЗИ, в зависимости от информации, содержащейся в информационной системе, целей создания информационной системы и задач, решаемых этой информационной системой, должны быть направлены на исключение:
неправомерных доступа, копирования, предоставления или

распространения информации (обеспечение конфиденциальности информации);

неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);

неправомерного блокирования информации (обеспечение доступности информации).

Процесс построения КСЗИ включает следующие этапы:

Формирование требований к защите информации, содержащейся в информационной системе.

Разработка КСЗИ информационной системы.
Внедрение КСЗИ информационной системы.

Аттестация информационной системы по требованиям защиты информации (далее - аттестация информационной системы) и ввод ее в действие.

Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы.

Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

Формирование требований к защите информации, содержащейся информационной системе

Формирование требований к защите информации, содержащейся в информационной системе, осуществляется обладателем информации с учетом ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» (далее - ГОСТ Р 51583) и ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования» (далее - ГОСТ Р 51624) и в том числе включает:

принятие решения о необходимости защиты информации, содержащейся в информационной системе;

классификацию информационной системы по требованиям защиты информации (далее - классификация информационной системы);

определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации; определение требований к системе защиты информации информационной системы.

1.1. При принятии решения о необходимости защиты информации, содержащейся в информационной системе, осуществляется:

Анализ целей создания информационной системы и задач, решаемых этой информационной системой.

Определение информации, подлежащей обработке в информационной системе.

Анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система.

Принятие решения о необходимости создания КСЗИ информационной системы, а также определение целей и задач защиты информации в информационной системе, основных этапов создания КСЗИ информационной системы и функций по обеспечению защиты информации,

содержащейся в информационной системе, обладателя информации.

1.2. Классификация информационной системы может проводиться в зависимости от значимости обрабатываемой в ней информации, способов еѐ обработки и масштаба информационной системы.
Требование к уровню (классу) защищенности включается в техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание КСЗИ информационной системы, разрабатываемые с учетом ГОСТ 34.602 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»

(далее - ГОСТ 34.602), ГОСТ Р 51583 и ГОСТ Р 51624.

Результаты классификации информационной системы оформляются актом классификации.

1.3. Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

При определении угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования.
По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик информационной системы, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Модель угроз безопасности информации содержит описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

1.4. Требования к системе защиты информации информационной системы

определяются в зависимости от уровня (класса) защищенности информационной системы и угроз безопасности информации, включенных в модель угроз безопасности информации.

Требования к системе защиты информации информационной системы включаются в техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание КСЗИ информационной системы, разрабатываемые с учетом ГОСТ 34.602, ГОСТ Р 51583 и ГОСТ Р 51624, и должны в том числе содержать:

цель и задачи обеспечения защиты информации в информационной системе;

класс защищенности информационной системы;

перечень нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система;

перечень объектов защиты информационной системы;

требования к мерам и средствам защиты информации, применяемым в информационной системе;

требования к защите информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями.

При определении требований к системе защиты информации информационной системы учитываются положения политик обеспечения информационной безопасности обладателя информации в случае их разработки по ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

2. Разработка КСЗИ информационной системы

Разработка КСЗИ информационной системы осуществляется в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным техническим заданием) на создание КСЗИ информационной системы с учетом ГОСТ 34.601 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» (далее - ГОСТ 34.601), ГОСТ Р 51583 и ГОСТ Р 51624 и в том числе включает:

Проектирование КСЗИ информационной системы.

Разработку эксплуатационной документации на систему защиты информации информационной системы.

Макетирование и тестирование КСЗИ информационной системы (при необходимости).

КСЗИ информационной системы не должна препятствовать достижению целей создания информационной системы и ее функционированию.

При разработке КСЗИ информационной системы учитывается ее информационное взаимодействие с иными информационными системами и информационно-телекоммуникационными сетями.

2.1. При проектировании КСЗИ информационной системы:

определяются типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (устройства, объекты файловой системы, запускаемые и исполняемые

модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа);

определяются методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток

безопасности, ролей и иных правил), подлежащие реализации в информационной системе;
выбираются меры защиты информации, подлежащие реализации в КСЗИ информационной системы;

определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;
определяется структура КСЗИ информационной системы, включая состав (количество) и места размещения ее элементов;
осуществляется выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих

средств и особенностей их реализации, а также класса защищенности информационной системы;
определяются параметры настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение

возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации;
определяются меры защиты информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

Результаты проектирования КСЗИ информационной системы отражаются в проектной документации (эскизном (техническом) проекте и (или) в рабочей документации) на информационную систему (систему защиты информации информационной системы), разрабатываемых с учетом ГОСТ 34.201 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» (далее - ГОСТ
34.201).

При отсутствии необходимых средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, организуется разработка (доработка) средств защиты информации и их сертификация в соответствии с законодательством Российской Федерации или производится корректировка проектных решений по информационной системе и (или) ее системе защиты информации с учетом функциональных возможностей имеющихся сертифицированных средств защиты информации.

2.2. Разработка эксплуатационной документации на систему защиты информации информационной системы осуществляется в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным техническим заданием) на создание КСЗИ информационной системы.
Эксплуатационная документация на КСЗИ информационной системы разрабатывается с учетом ГОСТ 34.601, ГОСТ 34.201 и ГОСТ Р 51624 и должна в том числе содержать описание:
структуры КСЗИ информационной системы;

состава, мест установки, параметров и порядка настройки средств защиты информации, программного обеспечения и технических средств;

правил эксплуатации КСЗИ информационной системы.

2.3. При макетировании и тестировании КСЗИ информационной системы в том числе осуществляются:

проверка работоспособности и совместимости выбранных средств

защиты информации с информационными технологиями и техническими средствами;

проверка выполнения выбранными средствами защиты информации требований к системе защиты информации информационной системы;

корректировка проектных решений, разработанных при создании информационной системы и (или) КСЗИ информационной системы;

корректировка проектной и эксплуатационной документации на систему защиты информации информационной системы.

3. Внедрение КСЗИ информационной системы

Внедрение КСЗИ информационной системы осуществляется в

соответствии с проектной и эксплуатационной документацией на систему защиты информации информационной системы и в том числе включает:

Установку и настройку средств защиты информации в информационной системе.

Разработку документов, определяющих правила и процедуры, реализуемые обладателем защищаемой информации для обеспечения защиты информации в информационной системе в ходе ее эксплуатации (далее - организационно-распорядительные документы по защите информации).

Внедрение организационных мер защиты информации.
Предварительные испытания КСЗИ информационной системы.
Опытную эксплуатацию КСЗИ информационной системы.
Анализ уязвимостей информационной системы и принятие мер защиты информации по их устранению.

Приемочные испытания КСЗИ информационной системы.

3.1. Установка и настройка средств защиты информации в информационной системе проводится в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и документацией на средства защиты информации.
3.2. Разрабатываемые организационно-распорядительные документы по защите информации определяют правила и процедуры:

управления (администрирования) системой защиты информации информационной системы;

выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования

информационной системы и (или) к возникновению угроз безопасности информации (далее - инциденты), и реагирования на них;
управления конфигурацией аттестованной информационной системы и КСЗИ информационной системы;

контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;

защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации.

3.3. При внедрении организационных мер защиты информации осуществляются:

реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий

эксплуатации, состава и конфигурации технических средств и программного обеспечения;
проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий

пользователей и администраторов информационной системы по реализации организационных мер защиты информации;

отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации.

Предварительные испытания КСЗИ информационной системы проводятся с учетом ГОСТ 34.603 «Информационная технология. Виды испытаний автоматизированных систем» (далее - ГОСТ 34.603) и включают проверку работоспособности КСЗИ информационной системы, а также принятие решения о возможности опытной эксплуатации КСЗИ информационной системы.

Опытная эксплуатация КСЗИ информационной системы проводится с учетом ГОСТ 34.603 и включает проверку функционирования КСЗИ информационной системы, в том числе реализованных мер защиты информации, а также готовность пользователей и администраторов к эксплуатации КСЗИ информационной системы.

3.6. Анализ уязвимостей информационной системы проводится в целях оценки возможности преодоления нарушителем КСЗИ информационной системы и предотвращения реализации угроз безопасности информации и

включает анализ уязвимостей средств защиты информации, технических средств и программного обеспечения информационной системы.
При анализе уязвимостей информационной системы проверяется отсутствие известных уязвимостей средств защиты информации, технических средств и программного обеспечения, в том числе с учетом информации, имеющейся у разработчиков и полученной из других общедоступных источников, правильность установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректность работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением.

В случае выявления уязвимостей информационной системы, приводящих к возникновению дополнительных угроз безопасности информации, проводится уточнение модели угроз безопасности информации

при необходимости принимаются дополнительные меры защиты информации, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителем выявленных уязвимостей.

Приемочные испытания КСЗИ информационной системы проводятся с учетом ГОСТ 34.603 и включают проверку выполнения требований к системе защиты информации информационной системы в соответствии с техническим заданием на создание информационной системы

(или) техническим заданием (частным техническим заданием) на создание КСЗИ информационной системы.

Аттестация информационной системы и ввод ее в действие
качестве исходных данных, необходимых для аттестации информационной системы, используются модель угроз безопасности информации, акт классификации информационной системы, техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание КСЗИ информационной системы, проектная и эксплуатационная документация на систему защиты информации информационной системы, организационно-распорядительные документы по защите информации, результаты анализа уязвимостей информационной системы, материалы предварительных и приемочных испытаний КСЗИ информационной системы.
Аттестация информационной системы проводится в соответствии с программой и методиками аттестационных испытаний до начала обработки информации, подлежащей защите в информационной системе. Для проведения аттестации информационной системы применяются национальные стандарты, а также методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16

августа 2004 г. N 1085.

По результатам аттестационных испытаний оформляются протоколы аттестационных испытаний, заключение о соответствии информационной системы требованиям о защите информации и аттестат соответствия в случае положительных результатов аттестационных испытаний.

Повторная аттестация информационной системы осуществляется в случае окончания срока действия аттестата соответствия или повышения класса защищенности информационной системы. При увеличении состава угроз безопасности информации или изменения проектных решений, реализованных при создании КСЗИ информационной системы, проводятся дополнительные аттестационные испытания в рамках действующего аттестата соответствия.

Ввод в действие информационной системы осуществляется в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации и с учетом ГОСТ 34.601 и при наличии аттестата соответствия.

5. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы

Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы осуществляется обладателем защищаемой информации в соответствии с эксплуатационной документацией на систему защиты информации и организационно-распорядительными документами по защите информации и в том числе включает:

управление (администрирование) системой защиты информации информационной системы;

выявление инцидентов и реагирование на них;

управление конфигурацией аттестованной информационной системы и ее КСЗИ;

контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в информационной системе.

5.1. В ходе управления (администрирования) системой защиты информации информационной системы осуществляются:

заведение и удаление учетных записей пользователей, управление

полномочиями пользователей информационной системы и поддержание правил разграничения доступа в информационной системе;

управление средствами защиты информации в информационной системе, в том числе параметрами настройки программного обеспечения, включая программное обеспечение средств защиты информации, управление

учетными записями пользователей, восстановление работоспособности средств защиты информации, генерацию, смену и восстановление паролей;

установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых

разработчиками (производителями) средств защиты информации или по их поручению;

централизованное управление системой защиты информации информационной системы (при необходимости);

регистрация и анализ событий в информационной системе, связанных с защитой информации (далее - события безопасности);

информированиепользователейобугрозахбезопасности
информации, о правилах эксплуатации КСЗИ информационной системы и отдельных средств защиты информации, а также их обучение;

сопровождение функционирования КСЗИ информационной системы в ходе ее эксплуатации, включая корректировку эксплуатационной

документации на нее и организационно-распорядительных документов по защите информации;

5.2. В ходе выявления инцидентов и реагирования на них
осуществляются:

определение лиц, ответственных за выявление инцидентов и реагирование на них;

обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору

информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

своевременное информирование лиц, ответственных за выявление

инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;

анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;
планирование и принятие мер по устранению инцидентов, в том числе по восстановлению информационной системы и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору

информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

планирование и принятие мер по предотвращению повторного возникновения инцидентов.

5.3. В ходе управления конфигурацией аттестованной информационной системы и ее КСЗИ осуществляются:

поддержание конфигурации информационной системы и ее КСЗИ (структуры КСЗИ информационной системы, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной
документацией на систему защиты информации (поддержание базовой конфигурации информационной системы и ее КСЗИ);

определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию информационной системы и ее КСЗИ;

управление изменениями базовой конфигурации информационной системы и ее КСЗИ, в том числе определение типов возможных изменений базовой конфигурации информационной системы и ее КСЗИ, санкционирование внесения изменений в базовую конфигурацию

информационной системы и ее КСЗИ, документирование действий по внесению изменений в базовую конфигурацию информационной системы и КСЗИ, сохранение данных об изменениях базовой конфигурации информационной системы и ее КСЗИ, контроль действий по внесению изменений в базовую конфигурацию информационной системы и ее КСЗИ;

анализ потенциального воздействия планируемых изменений в базовой конфигурации информационной системы и ее КСЗИ на обеспечение
защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность информационной системы;
определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и

конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию информационной системы и ее КСЗИ; внесение информации (данных) об изменениях в базовой

конфигурации информационной системы и ее КСЗИ в эксплуатационную документацию на систему защиты информации информационной системы;

принятие решения по результатам управления конфигурацией о

повторной аттестации информационной системы или проведении дополнительных аттестационных испытаний.
5.4. В ходе контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе, осуществляются:

контроль за событиями безопасности и действиями пользователей в информационной системе;
контроль (анализ) защищенности информации, содержащейся в информационной системе;

анализ и оценка функционирования КСЗИ информационной

системы, включая выявление, анализ и устранение недостатков в функционировании КСЗИ информационной системы;

периодический анализ изменения угроз безопасности информации в информационной системе, возникающих в ходе ее эксплуатации, и принятие

мер защиты информации в случае возникновения новых

угроз безопасности информации;

документирование процедур и результатов контроля (мониторинга)

за обеспечением уровня защищенности информации, содержащейся в информационной системе;

принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) КСЗИ информационной системы, повторной аттестации информационной системы или проведении дополнительных аттестационных испытаний.

6. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации

Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации осуществляется обладателем защищаемой информации в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и организационно-распорядительными документами по защите информации и в том числе включает:
Архивирование информации, содержащейся в информационной

системе.

Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

Архивирование информации, содержащейся в информационной системе, должно осуществляться при необходимости дальнейшего использования информации в деятельности обладателя защищаемой информации.

Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного

носителя информации другому пользователю информационной системы или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей информации.

Контрольные вопросы

Перечислите основные этапы построения КСЗИ.

Назовите ГОСТ с учѐтом которых должны быть разработаны требования к системе защиты информации.

Перечислите основные понятия которые будут определены при проектировании КСЗИ.

Перечислите основное содержание эксплутационной документации КСЗИ.
Перечислите этапы внедрения системы защиты информации.

Перечислите процессы выполняемые при обеспечении защиты информации в ходе эксплуатации аттестованной информационной системы.

Список индивидуальных тем
1. Банк
2. Больница
3. Юридическая фирма
4. Фирма, занимающаяся маркетинговыми исследованиями
5. Психологическая клиника
6. ЗАГС
7. УФМС
8. Казначейство
9. Радиозавод
10. Контора по ремонту и обслуживанию ПК
11. Налоговая инспекция
12. ВУЗ

13. УКЦ
14. Страховая компания
15. Дата-центр (ЦОД)
16. Интернет-провайдер
17. Сотовый оператор
18. Магазин бытовой техники
19. Аэропорт
20. Фирма по разработке ПО
21. Аптека
22. Склад, лучшее наверное система складских помещений
23. Железнодорожный вокзал
24. Электростанция
25. Управление дорожного хозяйства

Лабораторная работа 2.
Изучение методов комплексного исследование объекта информатизации

Цель работы: изучить положительные и отрицательные стороны проведения обследования защищенности объекта информатизации (ОИ) посредством существующих стандартов и методик.

Теоретическая часть

Известно, что при создании любой информационной системы (ИС) на базе современных компьютерных технологий неизбежно возникает вопрос о защищенности этой системы от угроз безопасности информации и принятия решения по устранению этих угроз. Однако для определения, как и от кого защищать информацию, необходимо уяснить реальное положение в области обеспечения безопасности информации и оценить степень защищенности ИС.

Для решения данной задачи проводится комплексное обследование защищенности ОИ, результаты которого основываются на выявленных угрозах безопасности информации и оценке рисков нанесения возможного ущерба, а также позволяют оценить необходимость и достаточность принятых на объекте мер обеспечения безопасности информации. Предполагается, что по результатам комплексного обследования ОИ определяются адекватные потребностям ИС (по степени защищенности ее ресурсов) требования к средствам ее защиты, что позволяет добиться максимальной отдачи от инвестиций в создание и обслуживание системы обеспечения информационной безопасности (СОИБ) ИС.
Задача проводимого обзора существующих стандартов и методик реализации обследования защищенности ОИ состоит в определении оценки объективности и полноценности данных стандартов и методик.

Если посмотреть на общую существующую классификацию видов обследования ИБ (обследования защищенности), то можно выделить три вида обследования защищенности:

инструментальное (дискретное и непрерывное);

обследование защищенности ОИ на соответствие существующим стандартам и методикам;

обследование защищенности как части специализированных исследований ОИ.

Перечень рассмотренных стандартов и методик, описывающих процессы обследования защищенности ОИ, представлены в стандартах ISO/IEC 15408, ISO/IEC 17799, ISO/IEC 27001:2005 и ISO/IEC 17799:2005 а

также руководящих документах ФСТЭК. Предполагается, что в результате комплексного обследования защищенности ОИ происходит выделение актуальных угроз безопасности информации и определение перечня контрмер – эффективных методов противодействия значимым угрозам. Однако проведенная оценка показывает, что четкое следование существующим стандартам и методам и, как следствие, объективность и полнота выдаваемых экспертных оценок в ходе проведения обследования защищенности во многом зависит от квалификации эксперта, проводящего обследование защищенности.

Таким образом, ставится актуальная в настоящее время задача по разработке механизма (и методики) обследования защищенности ОИ, способного выдавать обоснованные количественные оценки эффективности принятых мер противодействия, обоснованного количественного расчета деструктивных воздействий, проведения оценки угроз ОИ. Результатом применения разрабатываемого механизма должно стать снижение субъективности конечных оценок состояния защищенности ОИ и возможность обоснованной оценки эффективности принятых мер парирования угроз на ОИ.

Деятельность по аттестации объектов информатизации по требованиям безопасности информации осуществляет ФСТЭК России (бывш. Гостехкомиссия России). Для начала дадим определение объекта информатизации.

Объект информатизации - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

Аттестация объектов информатизации (далее аттестация) -

комплекс организационно-технических мероприятий, в результате которых посредством специального документа - "Аттестата соответствия" подтверждается, что объект соответствует требованиям стандартов или иных

нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России (Гостехкомиссией России). Наличие аттестата соответствия в организации дает право обработки информации с уровнем секретности (конфиденциальности) на период времени, установленный в аттестате.
Аттестация производится в порядке, установленном "Положением по аттестации объектов информатизации по требованиям безопасности информации" от 25 ноября 1994 года. Аттестация должна проводится до начала обработки информации, подлежащей защите. Это необходимо в целях официального подтверждения эффективности используемых мер и средств по защите этой информации на конкретном объекте информатизации.

Аттестация является обязательной в следующих случаях:
− государственная тайна;
− при защите государственного информационного ресурса;
− управление экологически опасными объектами; −
ведение секретных переговоров.
Во всех остальных случаях аттестация носит добровольный характер, то есть может осуществляться по желанию заказчика или владельца объекта информатизации.

Аттестация предполагает комплексную проверку (аттестационные испытания) объекта информатизации в реальных условиях эксплуатации. Целью является проверка соответствия применяемых средств и мер защиты требуемому уровню безопасности. К проверяемым требованиям относится:
− защита от НСД, в том числе компьютерных вирусов;
− защита от утечки через ПЭМИН;

защита от утечки или воздействия информацию за счет специальных устройств, встроенных в объект информатизации.
Аттестация проводится органом по аттестации в соответствии со схемой , выбираемой этим органом, и состоит из следующего перечня работ:
анализ исходных данных по аттестуемому объекту информатизации ;
предварительное ознакомление с аттестуемым объектом информатизации ;
проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте
точки зрения ее соответствия требованиям нормативной и методической документации;
проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;
проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;
проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;
анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение

заключения по результатам аттестации.
Органы по аттестации должны проходить аккредитацию ФСТЭК в соответствии с "Положением об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации".
Все расходы по проведению аттестации возлагаются на заказчика, как в случае добровольной, так и обязательной аттестации.
Органы по аттестации несут ответственность за выполнение своих функций, за сохранение в секрете информации, полученной в ходе аттестации , а также за соблюдение авторских прав заказчика.
В структуру системы аттестации входят:

− федеральный орган по сертификации средств защиты информации
аттестации объектов информатизации по требованиям безопасности информации – ФСТЭК России;
органы по аттестации объектов информатизации по требованиям безопасности информации;
испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации;
заявители (заказчики, владельцы, разработчики аттестуемых объектов информатизации).
качестве заявителей могут выступать заказчики, владельцы или разработчики аттестуемых объектов информатизации.
качестве органов по аттестации могут выступать отраслевые и региональные учреждения, предприятия и организации по защите
информации, специальные центры ФСТЭК России, которые прошли соответствующую аккредитацию.
Органы по аттестации:
− аттестуют объекты информатизации и выдают "Аттестаты соответствия ";
осуществляют контроль за безопасностью информации,
циркулирующей на аттестованных объектах информатизации, и за их эксплуатацией ;
отменяют и приостанавливают действие выданных этим органом "Аттестатов соответствия";
формируют фонд нормативной и методической документации, необходимой для аттестации конкретных типов объектов информатизации, участвуют в их разработке;

ведут информационную базу аттестованных этим органом объектов информатизации;
осуществляют взаимодействие с ФСТЭК России и ежеквартально информируют его о своей деятельности в области аттестации.
ФСТЭК осуществляет следующие функции в рамках системы аттестации:
организует обязательную аттестацию объектов информатизации;
создает системы аттестации объектов информатизации и устанавливает правила для проведения аттестации в этих системах;
устанавливает правила аккредитации и выдачи лицензий на проведение работ

по обязательной аттестации;
организует, финансирует разработку и утверждает нормативные и методические документы по аттестации объектов информатизации;
аккредитует органы по аттестации объектов информатизации и выдает им лицензии на проведение определенных видов работ;
осуществляет государственный контроль и надзор за соблюдением правил аттестации и эксплуатацией аттестованных объектов информатизации;
рассматривает апелляции, возникающие в процессе аттестации объектов информатизации, и контроля за эксплуатацией аттестованных объектов информатизации;
организует периодическую публикацию информации по функционированию системы аттестации объектов информатизации по требованиям безопасности информации.
Испытательные лаборатории проводят испытания несертифицированной продукции, используемой на аттестуемом объекте информатизации .

Со списком органов по аттестации и испытательных лабораторий, прошедших аккредитацию, можно ознакомиться на официальном сайте ФСТЭК России в разделе "Сведения о Системе сертификации средств защиты информации по требованиям безопасности информации".
Заявители:
проводят подготовку объекта информатизации для аттестации путем реализации необходимых организационно-технических мероприятий по защите информации;
привлекают органы по аттестации для организации и проведения аттестации объекта информатизации;
предоставляют органам по аттестации необходимые документы и условия для проведения аттестации;
привлекают, в необходимых случаях, для проведения испытаний несертифицированных средств защиты информации, используемых на аттестуемом объекте информатизации, испытательные центры (лаборатории) по сертификации;
осуществляют эксплуатацию объекта информатизации в соответствии с условиями и требованиями, установленными в "Аттестате соответствия";
извещают орган по аттестации, выдавший "Аттестат соответствия", всех изменениях в информационных технологиях, составе и размещении средств и систем информатики, условиях их эксплуатации, которые могут повлиять на эффективность мер и средств защиты информации (перечень характеристик, определяющих безопасность информации, об изменениях которых требуется обязательно извещать орган по аттестации, приводится в "Аттестате соответствия");
предоставляют необходимые документы и условия для осуществления контроля и надзора за эксплуатацией объекта информатизации, прошедшего обязательную аттестацию.
Для проведения испытаний заявитель предоставляет органу по аттестации следующие документы и данные:
− приемо-сдаточную документацию на объект информатизации;

акты категорирования выделенных помещений и объектов информатизации;

- инструкции по эксплуатации средств защиты информации;
- технический паспорт на аттестуемый объект;

документы на эксплуатацию (сертификаты соответствия требованиям безопасности информации) ТСОИ;
сертификаты соответствия требованиям безопасности информации на ВТСС;
сертификаты соответствия требованиям безопасности информации на технические средства защиты информации;

- акты на проведенные скрытые работы;

протоколы измерения звукоизоляции выделенных помещений и эффективности экранирования сооружений и кабин (если они проводились);
протоколы измерения величины сопротивления заземления;
протоколы измерения реального затухания информационных сигналов до мест возможного размещения средств разведки;
данные по уровню подготовки кадров, обеспечивающих защиту информации;
данные о техническом обеспечении средствами контроля эффективности защиты информации и их метрологической поверке;
нормативную и методическую документацию по защите информации и контролю эффективности защиты.
Приведенный общий объем исходных данных и документации может уточняться заявителем в зависимости от особенностей аттестуемого объекта информатизации по согласованию с аттестационной комиссией.

пояснительную записку, содержащую информационную характеристику и организационную структуру объекта защиты, сведения об
организационных и технических мероприятиях по защите информации от утечки по техническим каналам;
перечень объектов информатизации, подлежащих защите, с указанием мест их расположения и установленной категории защиты;
перечень выделенных помещений, подлежащих защите, с указанием мест их расположения и установленной категории защиты;
перечень устанавливаемых ТСОИ с указанием наличия сертификата (предписания на эксплуатацию) и мест их установки;

- перечень устанавливаемых ВТСС с указанием наличия сертификата мест их установки;

перечень устанавливаемых технических средств защиты информации с указанием наличия сертификата и мест их установки;
схему (в масштабе) с указанием плана здания, в котором расположены защищаемые объекты, границы контролируемой зоны, трансформаторной подстанции, заземляющего устройства, трасс прокладки
инженерных коммуникаций, линий электропитания, связи, пожарной и охранной сигнализации, мест установки разделительных устройств и т.п.;
технологические поэтажные планы здания с указанием мест расположения

объектов информатизации и выделенных помещений и
характеристиками их стен, перекрытий, материалов отделки, типов дверей и окон;
планы объектов информатизации с указанием мест установки
ТСОИ, ВТСС и прокладки их соединительных линий, а также трасс прокладки инженерных коммуникаций и посторонних проводников;
план-схему инженерных коммуникаций всего здания, включая систему вентиляции;
план-схему системы заземления объекта с указанием места расположения заземлителя;
план-схему системы электропитания здания с указанием места расположения разделительного трансформатора (подстанции), всех щитов и разводных коробок;
план-схему прокладки телефонных линий связи с указанием мест расположения распределительных коробок и установки телефонных аппаратов;
план-схему систем охранной и пожарной сигнализации с указанием мест установки и типов датчиков, а также распределительных коробок;
схемы систем активной защиты (если они предусмотрены). Порядок проведения аттестации объектов информатизации по требованиям безопасности информации включает следующие действия:
подача и рассмотрение заявки на аттестацию. Заявка имеет установленную форму, с которой можно ознакомиться в "Положении об аттестации объектов информатизации по требованиям безопасности". Заявитель направляет заявку в орган по аттестации, который в месячный срок рассматривает заявку, выбирает схему аттестации и согласовывает ее с заявителем.
предварительное ознакомление с аттестуемым объектом – производится в случае недостаточности предоставленных заявителем данных до начала аттестационных испытаний;
испытание в испытательных лабораториях несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте.

разработка программы и методики аттестационных испытаний. Этот шаг является результатом рассмотрения исходных данных и предварительного ознакомления с аттестуемым объектом. Орган по аттестации определяет перечень работ и их продолжительность, методику испытаний, состав аттестационной комиссии, необходимость использования контрольной аппаратуры и тестовых средств или участия испытательных лабораторий. Программа аттестационных испытаний согласовывается с заявителем.
заключение договоров на аттестацию. Результатом предыдущих четырех этапов становится заключение договора между заявителем и
органом по аттестации, заключением договоров между органом по аттестации и привлекаемыми экспертами и оформлением предписания о допуске аттестационной комиссии к проведению аттестации.
проведение аттестационных испытаний объекта информатизации.
ходе аттестационных испытаний выполняется следующее:
анализ организационной структуры объекта информатизации, информационных потоков, состава и структуры комплекса технических

средств и программного обеспечения, системы защиты информации на mобъекте, разработанной документации и ее соответствия требованиям нормативной документации по защите информации;
определяется правильность категорирования объектов ЭВТ и классификации АС (при аттестации автоматизированных систем), выбора и
применения сертифицированных и несертифицированных средств и систем защиты информации;
проводятся испытания несертифицированных средств и систем
защиты информации на аттестуемом объекте или анализ результатов их испытаний в испытательных центрах (лабораториях) по сертификации;
проверяется уровень подготовки кадров и распределение

ответственности персонала за обеспечение выполнения требований по безопасности информации;
проводятся комплексные аттестационные испытания объекта информатизации в реальных условиях эксплуатации путем проверки
фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;
оформляются протоколы испытаний и заключение по результатам аттестации с конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты объекта информатизации в соответствие с установленными требованиями и совершенствованию этой
системы, а также рекомендациями по контролю за функционированием объекта информатизации.
К заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод.
Протокол аттестационных испытаний должен включать:

- вид испытаний;
- объект испытаний;
- дату и время проведения испытаний;
- место проведения испытаний;

перечень использованной в ходе испытаний аппаратуры
(наименование, тип, заводской номер, номер свидетельства о поверке и срок его действия);
перечень нормативно-методических документов, в соответствии с которыми проводились испытания;

- методику проведения испытания (краткое описание);
- результаты измерений;
- результаты расчетов;

выводы по результатам испытаний

Протоколы испытаний подписываются экспертами – членами аттестационной комиссии, проводившими испытания, с указанием должности, фамилии и инициалов.
Заключение по результатам аттестации подписывается членами аттестационной комиссии, утверждается руководителем органа аттестации и

представляется заявителю [2]. Заключение и протоколы испытаний подлежат утверждению органом по аттестации.

оформление, регистрация и выдача "Аттестата соответствия" (если заключение по результатам аттестации утверждено).

осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации;

рассмотрение апелляций. В случае, если заявитель не согласен с отказом в выдаче "Аттестата соответствия", он может подать апелляцию в вышестоящий орган по аттестации или в ФСТЭК. Апелляция рассматривается в срок, не превышающий один месяц с привлечением заинтересованных сторон.

Аттестат соответствия должен содержать:

− регистрационный номер;
− дату выдачи;
− срок действия;
− наименование, адрес и местоположение объекта информатизации;
− категорию объекта информатизации;
− класс защищенности автоматизированной системы; − гриф секретности (конфиденциальности) информации,

обрабатываемой на объекте информатизации;

− организационную структуру объекта информатизации и вывод об уровне подготовки специалистов по защите информации;

− номера и даты утверждения программы и методики, в соответствии которыми проводились аттестационные испытания;

перечень руководящих документов, в соответствии с которыми проводилась аттестация;

номер и дата утверждения заключения по результатам аттестационных испытаний;

состав комплекса технических средств обработки информации ограниченного доступа, перечень вспомогательных технических средств и систем, перечень технических средств защиты информации, а также схемы

их размещения в помещениях и относительно границ контролируемой зоны, перечень используемых программных средств;

организационные мероприятия, при проведении которых разрешается обработка информации ограниченного доступа;

перечень действий, которые запрещаются при эксплуатации объекта информатизации;

список лиц, на которых возлагается обеспечение требований по защите информации и контроль за эффективностью реализованных мер и средств защиты информации.

Аттестат соответствия подписывается руководителем аттестационной комиссии и утверждается руководителем органа по аттестации.

Аттестат соответствия выдается на период, в течение которого обеспечивается неизменность условий функционирования объекта информатизации и технологии обработки защищаемой информации, могущих повлиять на характеристики, определяющие безопасность

информации (состав и структура технических средств, условия размещения, используемое программное обеспечение, режимы обработки информации, средства и меры защиты), но не более чем на 3 года.

Практическое задание

Написать отчѐт исследования предприятия, закреплѐнного на ЛР1, содержащий общие сведения о предприятии, о его деятельности и организационной структуре.

Изучить стандарты ГОСТ Р ИСО/МЭК 15408-1-2008, ГОСТ Р ИСО/МЭК 15408-2-2008, ГОСТ Р ИСО/МЭК 27001-2006, ГОСТ Р ИСО/МЭК 17799-2005

Контрольные вопросы

Какие существуют виды обследования защищѐнности?

Что должен содержать аттестита соответствия?

Назовите порядок проведения аттестации объектов информатизации по требованиям безопасности информации?

Какие документы предоставляет заявитель Для проведения испытаний органу по аттестации?

Какие функции осуществляет ФСТЭК в рамках системы аттестации?

Лабораторная работа 3.

Изучение информации циркулирующей в корпоративной информационной системе

Цель работы: научиться анализировать информацию, циркулирующую в корпоративной информационной системе, научиться строить диаграмму информационных потоков.

Теоретическая часть

1. Формирование баз данных архивов территориальных фондов корпоративных информационных систем.

В 1997 году Системой управления ресурсами Ханты-Мансийского автономного округа было принято решение о создании в территориальном геологическом фонде цифрового архива первичной геолого-геофизической информации.

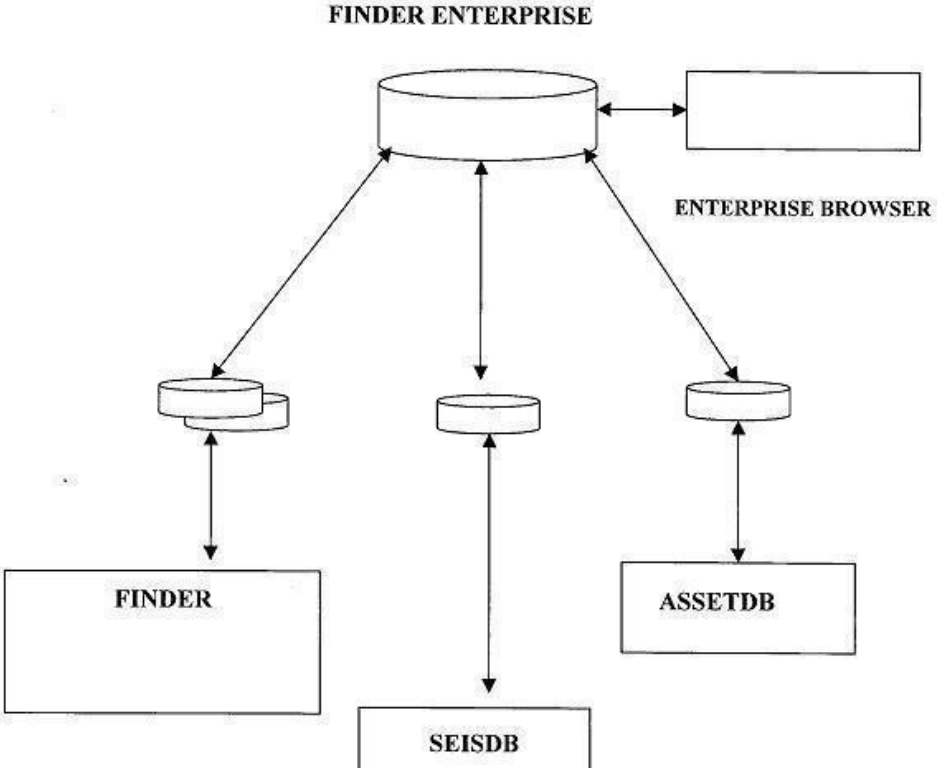
При создании архива использовались программные продукты фирмы Schlumberger GeoQuest: Finder, SeisDB и AssetDB. Все программное обеспечение функционирует под управлением СУБД ORACLE. На рис.1 представлена схема взаимодействия программного обеспечения, которое было использовано при создании архива.

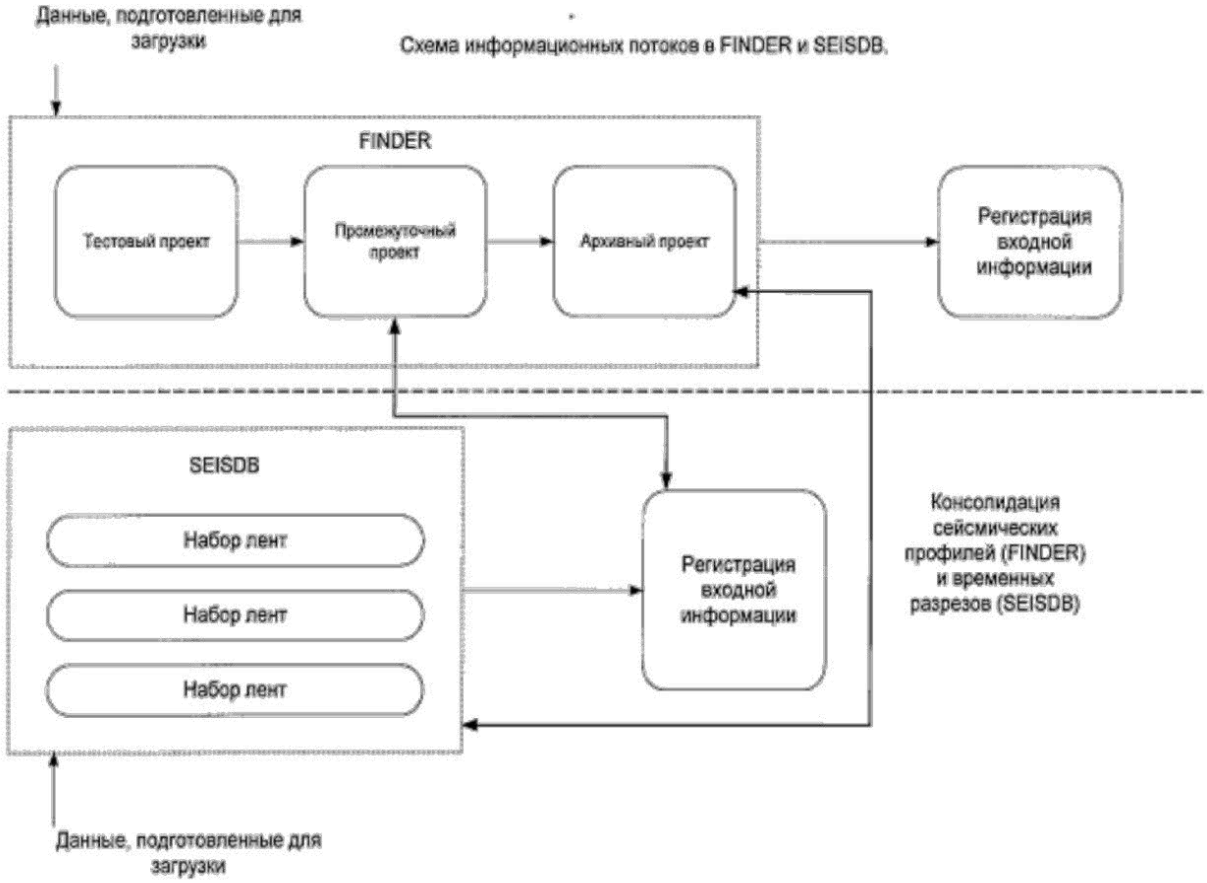
В настоящее время завершен первый этап реализации проекта — разработана модель данных архива. При составлении модели данных за основу был взят утвержденный «Регламент организации информационных потоков данных сейсморазведки», в котором перечислены все типы информации, предназначенные для хранения в архиве, и описаны форматы этих данных.

О модели: Исходные файлы каталогизируются и хранятся в оригинальном виде. Для этого с поступающих на хранение файлов собирается идентификационная информация: оригинальное имя файла, тип содержащейся в нем информации и т.п. и заносится в специальную таблицу –

каталог. Для работы с этим каталогом разработана специальная форма регистрации поступающей информации, позволяющая при необходимости легко найти и идентифицировать каждый конкретный файл.
Информация, с которой программное обеспечение работает в собственных форматах, также помещается в специальные структуры:
полевые записи после демультиплексации в формате SEG-Y, окончательные временные разрезы и разрезы ОГТ в сохраненных амплитудах загружаются в систему архивирования SeisDB;
общая информация по съемке, координаты пунктов взрыва и ОГТ
по профилям, горизонты T0, V, H по профилям, карты в сетках (grid) загружаются в систему Finder.
На рис. 2 и 3 представлены схемы информационных потоков сейсмической информации и этапы прохождения исходных данных при загрузке их в архив. В течение 1998 года аппаратное и программное обеспечение полностью подготовлено к загрузке данных. Было организовано обучение специалистов ТГФ. Проведен контроль качества и анализ сейсмической информации,поступающей из различных источников. Как показывает опыт, в каждой организации существует своя специфика подготовки выходной информации. Разработан ряд дополнительных программ и процедур подготовки данных для загрузки в архив. В основном эти программы ориентированы на форматы данных, утвержденные в «Регламенте». Сейсмическая информация, удовлетворяющая требованиям «Регламента», загружена в базы данных (Finder и SeisDB). В течение 1998 года в ТГФ был сдан материал на магнитных носителях по 12 сейсмопартиям. Был проведен контроль качества информации и загрузка в базу данных проверенного материала.

Рис. 1 Схема взаимодействия программного обеспечения





В базу данных загружена информация по:

- временным разрезам – 71;
- сейсмопрофилям – 219;

подготовлен к загрузке и частично загружен материал по 7 сейсмопартиям ; окончательно загружен и консолидирован материал по 1 сейсмопартии .

Проведен контроль качества и анализ существующих и поступающих данных ГИС. Разработан ряд дополнительных процедур, позволяющих проводить контроль качества, подготовку и загрузку данных ГИС в пакетном режиме. Загружено кривых: 38 тыс. по 950 скважинам. Эта работа продолжается по мере поступления информации. На рисунке 4 представлены этапы подготовки и загрузки в базу данных Finder информации по ГИС.

Программное обеспечение AssetDB используется для ведения журнала регистрации машинных носителей. Созданы необходимые для этого формы отчетных документов.
Кроме того, основными задачами территориального фонда геологической информации являются:

− государственная регистрация работ по геологическому изучению недр, выполняемых всеми организациями и предприятиями на территории Ханты-Мансийского автономного округа в соответствии с планами ГРР предприятий;
− государственный учет работ по геологическому изучению недр, сбор, систематизация и хранение неопубликованной геологической информации. территориальном фонде создана база данных под управлением СУБД ORACLE для учета зарегистрированных работ и ведения картотеки отчетов и дел скважин, принятых на хранение в ТГФ. На рис. 5 и 6 представлены формы регистрации и учета дел скважин и сейсмических отчетов.
настоящее время в территориальный фонд геологической информации принято и поставлено на учет 2011 единиц хранения фондовых материалов, в том числе 1085 единиц по скважинам глубокого бурения, 236 сейсмических отчетов и 690 отчетов по тематическим работам.

Рис.5 Окно программы.

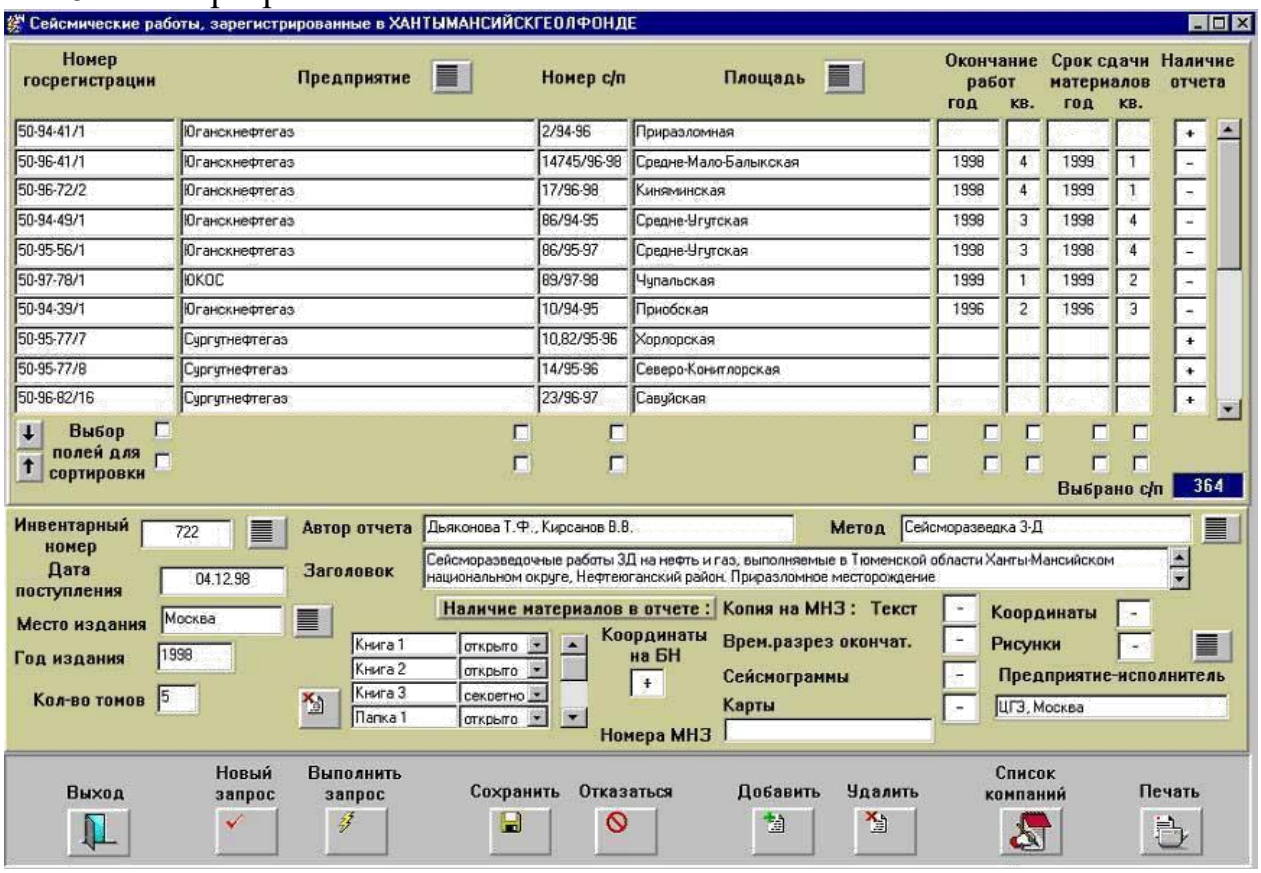


Рис.6 Окно программы.

2. Моделирование и анализ корпоративных информационных систем

Успешное развитие любого современного предприятия (корпорации) во многом зависит от его информационной системы (ИС) - от того, как она создавалась, как развивается и как осуществляется ее поддержка. При этом под ИС понимается совокупность всей информации, используемой в работе предприятия, и комплекса программно-технических, методических и организационных компонентов, обеспечивающих создание, обработку, передачу и прием этой информации.

Среди основных требований, которые предъявляются к ИС, можно назвать следующие.

Адекватность. ИС должна соответствовать задачам, для решения которых она создана или создается.

Масштабируемость. Эту адекватность ИС должна сохранить при развитии организационной структуры и росте информационной нагрузки, не требуя при этом серьезного изменения архитектуры системы.

Расширяемость. Нужно, чтобы ИС могла развиваться, позволяя исключать и модифицировать старые, добавлять новые компоненты, что должно обеспечиваться резервами стационарных систем (например, резервом ресурсов и 15-летней гарантией работоспособности структурированной кабельной сети).

Надежность. Сбои в работе критически важных приложений, простой которых приводит к финансовым потерям, недопустимы.

Сохранность инвестиций. При модификации системы следует

максимально использовать ранее приобретенное и установленное оборудование и имеющиеся компоненты системы.
Экономическая эффективность. Прибыль (непосредственная или косвенная), получаемая за счет использования ИС, должна превышать затраты на создание и развитие ИС.
Безопасность. Необходимо обеспечить защиту ИС от некорректных
или неавторизованных действий пользователей, от несанкционированного доступа.
Поэтапную схему создания и эксплуатации ИС можно нарисовать следующим образом: требования заказчика - замысел разработчика - проектирование - внедрение и обслуживание - анализ - модернизация. На этапе проектирования ИС закладывается обеспечение всех перечисленных выше требований.

В настоящее время при проектировании и сопровождении ИС чаще всего используется **технология** экспертных оценок. Главным определяющим фактором при таком подходе является опыт разработчиков и системных администраторов , а основной его недостаток состоит в субъективности.
Устранить этот недостаток можно с помощью технологий моделирования. Построение модели, ее анализ и отработка ситуаций ―что будет, если?..‖ позволяют смоделировать основные процессы, которые будут происходить в системе, и избежать экстремальных ситуаций. Моделирование может быть физическим - с использованием стендов (макетирование) или компьютерным, основанным на применении систем моделирования. Последнее позволяет существенно сэкономить силы и время команды разработчиков, а также достичь максимального соответствия проектируемой ИС предъявляемым заказчиком требованиям. При этом компьютерное моделирование требует гораздо меньших инвестиций и позволяет просмотреть больше вариантов, чем при физическом моделировании.
На первый взгляд может показаться, что на этапе внедрения и обслуживания, а также при работе ИС в установившемся режиме потребность в моделировании исчезает. Но при возникновении сбоев в работе ИС, изменении организационной структуры компании, использовании новых технологических решений (например, внедрении программных систем типа клиент-сервер), замене устаревающего оборудования и т. д. именно
система моделирования поможет ответить, например, на вопрос, как повлияет модернизация на существующую ИС и как провести эту модернизацию наилучшим образом?
При этом задача обеспечения предъявляемых к ИС требований почти целиком возлагается на системных администраторов, осуществляющих ее сервис и управление. Посмотрим, что же подразумевается под управлением ИС.

− Постоянный мониторинг системы. Для этой цели применяются системы мониторинга, управления сетями, а также анализаторы трафика
(такие, как IBM NetView, HP OpenView, Cabletron Spectrum, Expert Sniffer, NETscout и др.), которые служат источником информации о сетевой топологии и трафике существующей ИС.

− Принятие решений тактического и стратегического характера на основе данных, получаемых с помощью мониторинга. Именно от этих решений зависит оптимальное состояние ИС. Однако для их успешной выработки необходимо постоянно собирать и анализировать информацию от систем средств мониторинга.

И в этом случае моделирование ИС является эффективным инструментом решения проблемы. На основе собираемой информации строится (или модифицируется) модель ИС. В дальнейшем на этой модели можно отслеживать влияние изменений - как реально происходящих, так и предполагаемых по сценариям типа ―что будет, если?..‖.

Таким образом, моделирование позволяет реализовать в динамичном режиме схему ―замысел разработчика ИС - модель - верификация - реализация без ошибок‖ или ―существующее состояние ИС - модель - оптимальное состояние ИС‖. Рассмотрим, каким образом организуется такая взаимосвязь. ИС может быть представлена в виде четырехуровневой структуры (схема 1): коммуникационный (сетевые протоколы различных уровней, активное сетевое оборудование);

− уровень системного ПО (операционные системы);

уровень платформного (инструментального) ПО (СУБД, почтовые системы);

уровень прикладного ПО (собственно прикладные программные системы).

Однако в зависимости от степени абстрагирования это деление может быть сведено к двум уровням:

– уровень инфраструктуры;
– прикладной уровень.

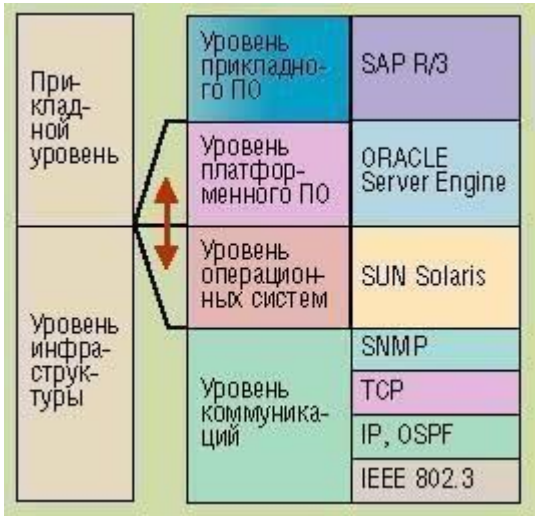


Схема 1. Уровни представления ИС Подобное деление отнюдь не является жестко заданным, а

определяется принятой нами степенью абстракции. На практике же оно показывает, насколько детально описаны объекты моделирования.
Исходные данные для построения модели предоставляет информация о топологии ИС (ее коммуникационной составляющей), о внутрисистемном трафике, зависящем от уровня и внутренних характеристик моделируемых объектов (аппаратной и программной составляющих). На основе анализа полученной модели можно прогнозировать поведение системы в описанном состоянии. При необходимости в модели отражаются вносимые изменения до их реального осуществления. Использование сценариев позволяет осуществлять детальный многовариантный анализ влияния вносимых изменений как в целом на ИС, так и на ее отдельные составляющие. Упрощается процесс установки нового распределенного программного обеспечения в реальную сеть, который также можно предварительно проанализировать с помощью модели существующей ИС. При этом могут быть выявлены потенциальные проблемы и найдены пути их устранения, не оказывающие какого-либо воздействия на реальную систему (схема 2.). Таким образом, из множества путей модификации системы с минимумом затрат может быть выбран оптимальный.

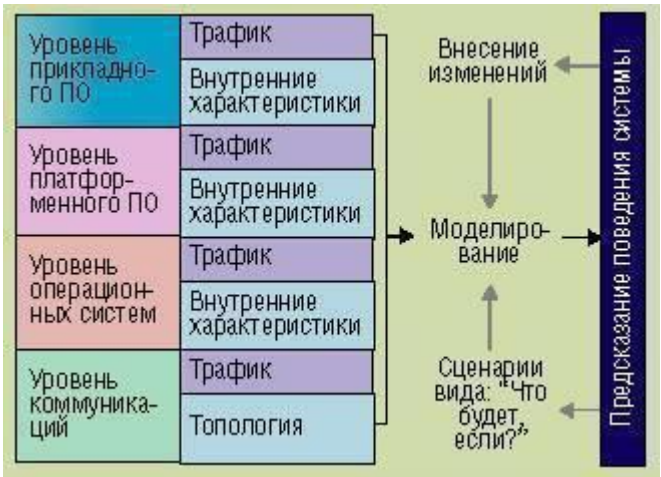


Схема 2. Моделирование ИС Моделирование представляется наиболее эффективным путем поддержания ИС в оптимальном состоянии по целому ряду параметров.

Экономическая эффективность модельного подхода не подлежит сомнению. Создание стендовых прототипов требует значительно больших инвестиций при существенно меньшей гибкости. Разработка ИС и внесение в ее изменений ―вслепую‖ несомненно обуславливает увеличение затрат.
Гибкий многовариантный анализ. При использовании модели ИС выбор между различными сетевыми технологиями (frame relay или ATM?), различным сетевым оборудованием (Cisco или Memotec?), транспортными протоколами (TCP или UDP?) находится ―на расстоянии одного щелчка мышью‖.

COMNET		OPNET	
Инструмент	**Назначение**	**Инст-румент**	**Назначение**
COMNET III	Детальное моделирование и анализ коммуникационных, компьютерных и программных систем	OPNET Modeler	Моделирование и анализ производительности сетей, компьютерных систем, приложений и распределенных систем
Distributed Software Module	Детальное моделирование распределенных программных систем		
Application Profiler	Создание профилей распределенных программных продуктов для дальнейшего анализа в COMNET III	OPNET Planner	Оценка производительности коммуникационных сетей и распределенных систем
Circuit-Switched Traffic Module	Детальное моделирование и анализ сетей X.25, frame relay и ATM		
COMNET Predictor*	Быстрая оценка и планирование производительности систем, прогнозирование их поведения	OPNET Xpress Developer	Инструмент для организации совместного моделирования в составе рабочей группы
COMNET Baseliner	Интерфейс с системами управления сетями и их мониторинга		
* Инструменту COMNET Predictor журнал Network Magazine присудил титул "Продукт года — 98".			

Состав систем моделирования COMNET и OPNET
− Возможность предсказания проблем до их реального возникновения также является исключительно важным достоинством моделирования, существенно повышающим надежность ИС, а следовательно, снижающим эксплуатационные расходы.
Кому же необходимо моделирование? На наш взгляд, прежде всего: разработчикам ИС, системным администраторам, специалистам служб безопасности.

Для разработчиков ИС, или, как их принято сейчас называть, проектных и системных интеграторов моделирование - это единственный способ получить объективное представление о работе системы до ее реального воплощения в жизнь. Причем это представление не ограничивается естественным вопросом, сколько это будет стоить. Результаты моделирования представляют собой источник конкретных цифр, конкретные показатели производительности, которые станут большим козырем в общении с заказчиком и позволят ответить на вопрос, как вложения заказчика в систему

могут себя оправдать. Кроме того, моделирование позволит разработчику системы избежать многих проблем на этапе реализации проекта и при последующем сопровождении.

Сеть, состоящая из десяти рабочих станций и одного файл-сервера на базе Microsoft Windows NT, не требует моделирования. Однако администратор большой системы, использующей различные стеки протоколов, операционные системы и распределенные приложения, зачастую сталкивается с трудно разрешаемыми проблемами, особенно при модернизации, например при установке приложения типа клиент-сервер или переходе с 10BaseT на 100VG AnyLAN. А как обстоят дела с прогнозами на будущее? Попытайтесь ответить на несколько вопросов. Можете ли вы, как администратор, предсказать прирост трафика в вашей системе за год, месяц, квартал? Каким образом этот прирост повлияет на вашу сеть? Не возникнут ли при этом узкие места? Ответы вы сможете получить, лишь построив модель системы и подвергнув ее детальному анализу.

В данном контексте мы считаем необходимым выделить в отдельную категорию специалистов и администраторов служб безопасности. Связано это с тем, что сегодня во многих организациях существует два реальных центра управления: администратор сети и администратор **безопасности**. Естественно, что такая ситуация приводит к рассогласованности действий. В результате встает вопрос об администрировании без вмешательства в настройки системы. А для этого необходим продукт, позволяющий собирать статистические данные о системном трафике за определенный период времени (направленность, приложение, протокол, распределение во времени и т. д.), а затем производить их анализ на модели.

Современный рынок предлагает широкий спектр программных продуктов, позиционируемых как средства моделирования информационных систем и сетей. Мы остановимся на двух, на наш взгляд, наиболее интересных: COMNET (CACI Products Company, США) и OPNET (MIL3,
США). Рассмотрим основные инструменты, входящие в состав этих систем. Оба продукта можно отнести примерно к одной категории. Сфера их применения - детальное моделирование сложных информационных систем, быстрая оценка производительности, прогнозирование реакции на вносимые изменения. Каким же образом осуществляется моделирование с помощью COMNET и OPNET?

Модель состоит из двух частей: описания топологии информационной системы и данных о трафике. Эта информация может быть либо получена из внешних источников - систем мониторинга и управления сетями, либо введена непосредственно пользователем с помощью интуитивно понятного графического интерфейса.

Определим базовые понятия, которые мы будем использовать в дальнейшем при описании технологий моделирования.

Под топологией понимается связный граф, в вершинах которого расположены узлы (node) - объекты с описанием аппаратного обеспечения (компьютеров и сетевого оборудования со своими характеристиками). системе COMNET, кроме того, в вершинах графа размещаются соединения (link), описывающие технологии передачи данных и осуществляющие обмен

информацией между узлами. Дуги (arcs), образующие граф, связывают узлы и соединения, определяя, какие узлы используют то или иное соединение. Фактически дуги представляют собой порты оборудования, расположенного в вершинах графа.

системе OPNET технологии передачи данных описываются непосредственно дугами, соединяющими вершины (узлы).
Кроме узлов и соединений для описания иерархических топологий и для моделирования независимых маршрутизируемых доменов в системе COMNET имеются два дополнительных объекта, которые также могут располагаться в вершинах графа - подсеть (subnet) для описания сложных иерархических структур и транзитная сеть (transit net) - сеть, параметры которой неизвестны или их описание не требуется. Для построения моделей глобальных сетей предназначен объект облако (WAN cloud). Эти три дополнительных объекта содержат свою собственную внутреннюю топологическую структуру. В системе OPNET для описания маршрутизации и иерархических структур используются также объекты ―подсеть‖ и другие способы (например, объект OSPF area).
Трафик будем рассматривать как количественную характеристику, описывающую информационные потоки между вершинами графа и распределенную во времени в соответствии со статистическими законами.
Описание трафика в COMNET выполняется с помощью таких объектов, как сообщение (message), сессия (session), отклик (response), вызов (call). Для них могут быть заданы законы, по которым описываются распределение моделируемого информационного потока во времени и количественные характеристики передаваемой информации.
Еще одним источником трафика, который мы намеренно выделяем в отдельную группу, являются распределенные программные системы. Для их моделирования в COMNET введен отдельный объект приложение (application). Использование этого объекта позволяет моделировать сложные программные комплексы, их взаимодействие с такими характеристиками узлов (processing node), как параметры жестких дисков и файловой системы, а также взаимодействие между различными приложениями.
На рис. 2.1 приведен пример главного окна и модели системы COMNET.

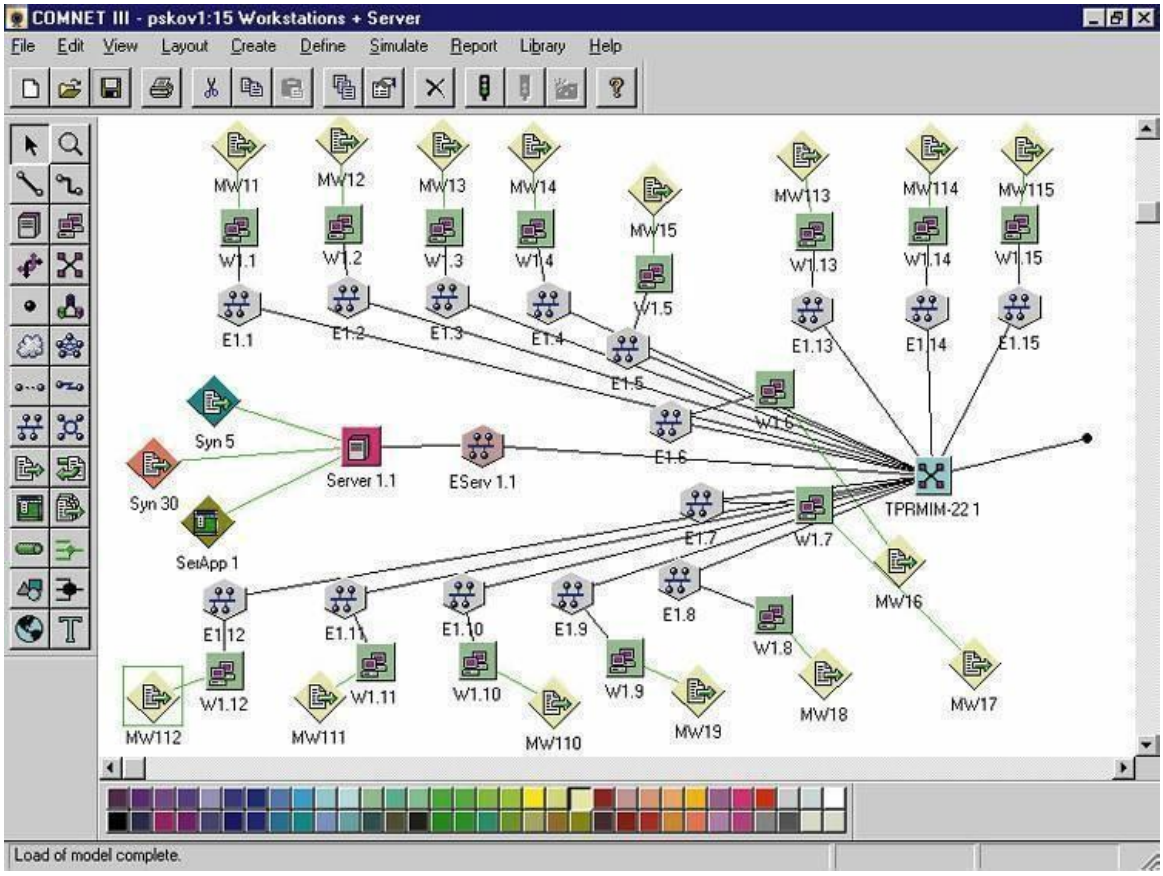


Рис. 2.1. Главное окно системы COMNET

В системе OPNET трафик задается другим способом: с помощью ―датчиков‖ (probe) данных, которые подключаются к определенным вершинам графа топологии и позволяют генерировать и собирать данные, а также описывать различные типы источников трафика (запросы, отклики, приложения). При этом имеется возможность задавать законы распределения параметров.

Главное окно системы OPNET приведено на рис. 2.2.

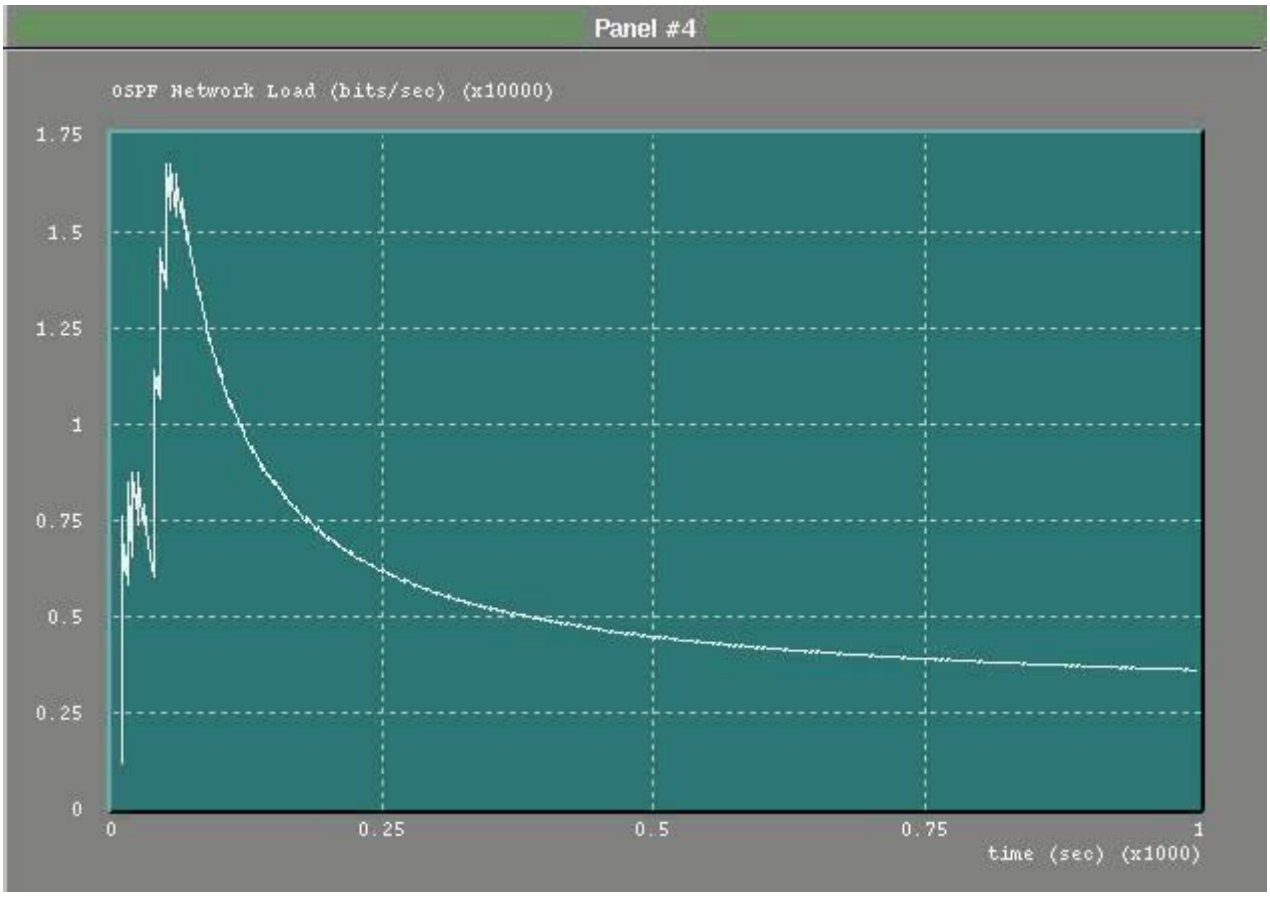


Рис. 2.2. Главное окно системы OPNET

Результаты моделирования представляются в текстовой и графической формах, удобных для дальнейшего анализа (рис. 3).

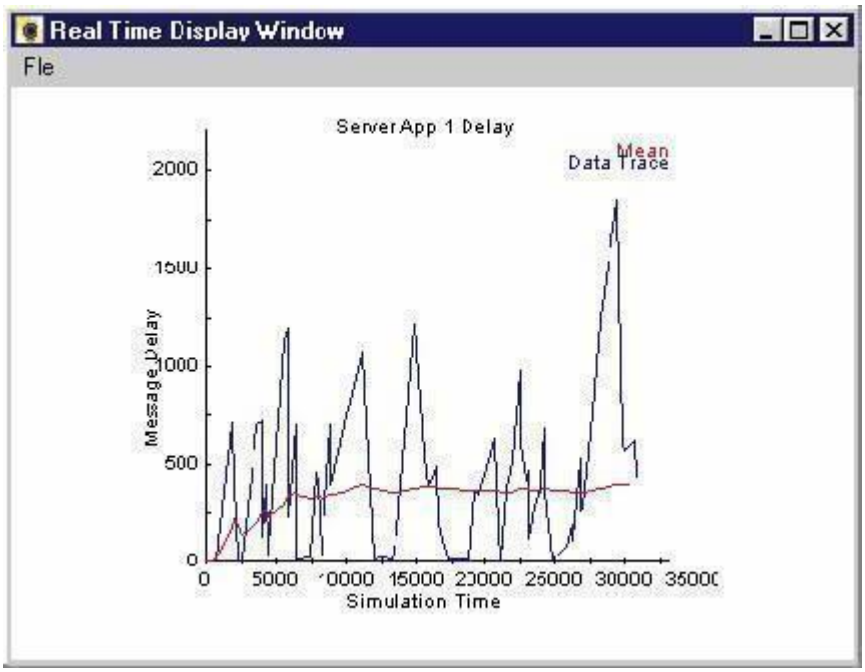


Рис. 2.3. Графическое представление результатов моделирования

Итак, мы рассмотрели основные понятия и конструктивные блоки, при помощи которых производится описание модели ИС в системах моделирования COMNET и OPNET. В дальнейших публикациях предполагаем остановиться на следующих вопросах:

Требования к программному и аппаратному

Аппаратная платформа	Операционная система	Объем ОЗУ, Мб	Дисковое пространство, Мб
IBM PC	Microsoft Windows 95/NT 4.0	32	50
SPARC	Solaris 2.5, SunOS 5.5	64	50
HP 9000/700	HP-UX 10.20	64	50
SGI O2	IRIX 6.3	64	50

- обеспечению системы COMNET
- технология моделирования в системе COMNET;
- моделирование и анализ сетей на основе Microsoft Windows NT;

моделирование и анализ распределенных систем обработки и хранения данных;
- моделирование и анализ систем видеоконференций;
- моделирование систем групповой работы и почтовых систем; решение проблем маршрутизации в сетях с использованием средств моделирования ;
- моделирование и анализ глобальных сетей;
- моделирование и анализ беспроводных технологий; моделирование и анализ медицинских информационных систем.

Аппаратная платформа	Операционная система	Объем ОЗУ, Мб	Дисковое пространство, Мб
IBM PC	Microsoft Windows NT 4.0	32	209**
SPARC	Solaris 2.3, SunOS 4.1.4	32	182
HP 9000/700	HP-UX 10.20	32	182
SGI O2	IRIX 6.3	32	182
DEC Alpha	OSF/1 3.0	32	182
* Помимо перечисленных параметров OPNET требует наличия в системе пользователя ANSI C Compiler (UNIX) либо Microsoft Visual C/C++ версии 4.x или выше (Windows NT). ** Для работы под управлением Microsoft Windows NT требуется файловая система NTFS.			

Требования к программному и аппаратному обеспечению системы

OPNET *

Практическое задание

Ознакомиться с теоритическим материалом.

Построить алгоритм анализа информации, циркулирующей в корпоративной информационной системе.

Проанализировать информацию, циркулирующей в корпоративной информационной системе предприятия.

Построить полную диаграмму информационных потоков предприятия.

Контрольные вопросы

Что представляет диаграмма информационных потоков?

Какие элементы должны быть отображены на диаграмме информационных потоков?

Какое программное обеспечение может быть использовано для построения диаграммы информационных потоков?

Какие принципы используется для построения диаграммы информационных потоков?

Что представляет собой полная диаграмма информационных потоков?

Лабораторная работа 4.

Изучение построения системы защиты информации на основе нормативных актов и методических указаний

Цель работы: изучить перечень нормативных документов на основе которых осуществляется построение системы защиты информации.

Теоретическая часть

Защита информации является составной частью работ по созданию и эксплуатации объектов информатизации различного назначения и осуществляется в соответствии с установленным руководящими документами порядком в виде системы (подсистемы) защиты информации. Защите подлежит информация, как речевая, так и обрабатываемая техническими средствами, а также представленная в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, оптической и иной основе, в виде информационных массивов и баз данных в автоматизированной системе.

Защита конфиденциальной информации осуществляется на основании федеральных законов «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене», Указа Президента Российской Федерации от 06.03.1997 г. № 188 «Перечень сведений конфиденциального характера», «Доктрины информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации 09.09.2000 г. № Пр.-1895, других нормативных правовых актов по защите информации, а также опыта реализации мер защиты информации в министерствах и ведомствах, в учреждениях и на предприятиях.

В качестве примера рассмотрим одну из наиболее важных задач, решаемых в области защиты информации, – обеспечение безопасности персональных данных граждан. Для того чтобы ее решить, необходимо не только

придерживаться порядка, установленного нормативными и методическими документами, но и хорошо ориентироваться в том, что касается классификации информационных систем и категорий персональных данных, применяемых технологий и средств защиты.

Основным законодательным актом в области защиты персональных данных является Федеральный закон № 152-ФЗ «О персональных данных» от 27.07.2006 г. Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой органами государственной власти, иными государственными органами, юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств.

В соответствии с законом «О персональных данных» уполномоченные органы с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливают:
уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;
требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Уровень защищѐнности персональных данных определяется на этапе классификации информационной системы персональных данных в соответствии с Постановлением Правительства № 1119 «Об утверждении

требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 г. Устанавливаются 4 уровня защищѐнности персональных данных в зависимости от категории данных, количества субъектов персональных данных и типа угроз безопасности персональных данных, актуальных для системы. К каждому из четырех уровней предъявляются общие требования к защите данных.

Формирование конкретных требований к системе защиты информации (персональных данных) осуществляют в соответствии с приказом ФСТЭК № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 г.

Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных описаны в Постановлении Правительства № 512 от 06.07.2008 г. «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

Требования к процессу обработки персональных данных, осуществляемому без использования средств автоматизации, установлены Постановлением Правительства № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 г.

Все описанные выше законодательные акты и нормативные документы в области защиты персональных данных содержат описание организационных и технических мер обеспечения безопасности персональных данных за исключением требований, предъявляемых в случае использования криптографических (шифровальных) средств.

В случае применения криптографических средств защиты информации, их разработка, внедрение и эксплуатация осуществляется в соответствии с «Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденными приказом ФСБ № 149/54-144 от 21.02.2008 г., а также в соответствии с «Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденными приказом ФСБ № 149/6/6-622 от 21.02.2008 г.

При построении модели угроз и модели вероятного нарушителя безопасности информации (персональных данных) применяют «Методику определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», а также «Базовую модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

Для учреждений здравоохранения, социальной сферы, труда и занятости составлен документ «Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости».

Таким образом, каждый из этапов построения комплексной системы защиты информации регламентируется определенными законодательными и нормативными актами Правительства РФ, ФСТЭК и ФСБ, определяющими порядок и методику создания системы защиты информации, требования к

ней, а также содержание организационных и технических мер по обеспечению безопасности информации.

Таким образом, создание системы защиты информации на примере системы защиты персональных данных на различных этапах осуществляется в соответствии со следующими законодательными актами и нормативно-методическими документами:

Федеральный закон № 152-ФЗ «О персональных данных» от 27.07.2006 г.

Постановление Правительства № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 г.

Приказ ФСТЭК № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 г.

Постановление Правительства № 512 от 06.07.2008 г. «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

Постановление Правительства № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 г.

«Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утверждены приказом ФСБ № 149/54-144 от 21.02.2008 г.

«Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности

персональных данных при их обработке в информационных системах персональных данных», утверждены приказом ФСБ № 149/6/6-622 от 21.02.2008 г.
«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».
«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».
10. «Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости».

Практическое задание

Составить перечень мероприятий необходимых для построения КСЗИ с учѐтом нормативно-методических актов.

Контрольные вопросы

Назовите закон о защите персональных данных.

Каким документом определяются требования к защите персональных данных?

Назовите перечень документов используемых для защиты персональных данных.

Назовите документ регламентирующий использование криптографических средств защиты в информационных системах.

Лабораторная работа 5.
Построение модели угроз ИСПДн

Цель работы: изучить нормативные документы ФСТЭК по построению модели угроз. Построить модель угроз информационной системы персональных данных функционирующей в Вашей организации.

Теоретическая часть

В соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» разработанной ФСТЭК, определение уровня исходной защищѐнности производится на основании анализа технических и эксплуатационных характеристик ИСПДн. Характеристики, необходимые для определения уровня защищѐнности ИСПДн приведены в таблице 1.

Исходный уровень защищенности определяется следующим образом:

ИСПДн имеет *высокий* уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).

ИСПДн имеет *средний* уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.

ИСПДн имеет *низкую* степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

При составлении перечня актуальных угроз безопасности ПДн каждой

степени исходной защищенности ставится в соответствие числовой коэффициент Y_1, а именно:
– для высокой степени исходной защищенности;
– для средней степени исходной защищенности;
– для низкой степени исходной защищенности.
Характеристики для определения исходного уровня защищѐнности ИСПДн приведены в таблице 2.

Определение вероятности реализации угроз безопасности в информационной системе персональных данных

В соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» разработанной ФСТЭК, под *частотой (вероятностью) реализации угрозы* понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки.
Вводятся четыре вербальных градации показателя «Вероятность реализации угрозы»:
маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации
лицами, не имеющими легального доступа в помещение, где последние хранятся);
низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);
средняя вероятность – объективные предпосылки для реализации
угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны ;
высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.
При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y_2, а именно:

0 – для маловероятной угрозы;
2 – для низкой вероятности угрозы;
5 – для средней вероятности угрозы;
10 – для высокой вероятности угрозы.

Определение коэффициента реализуемости угрозы.

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением (1)

$$= (_1 + _2)/20 \quad (1)$$

Где: 1 − коэффициент защищённости ИСПДн; 2 − вероятность возниконовыния угрозы.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

− если $0 \le Y \le 0{,}3$, то возможность реализации угрозы признается низкой;

− если $0{,}3 < Y \le 0{,}6$, то возможность реализации угрозы признается средней;

− если $0{,}6 < Y \le 0{,}8$, то возможность реализации угрозы признается высокой;

− если $Y > 0{,}8$, то возможность реализации угрозы признается очень высокой.

Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИСПДн. Этот показатель имеет три значения:

– низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

– средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

– высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных. Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами, приведенными в таблице 1.

Таблица 1 Правила отнесения угрозы безопасности ПДн к актуальной

Возможность реализации угрозы	***Показатель опасности угрозы***		
	Низкая	***Средняя***	***Высокая***
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

На основании экспертных оценок вероятности реализации угроз и показателя опасности, с учетом коэффициента исходной защищенности ИСПДн рассчитывается степень актуальности угроз безопасности ПДн.

Практическое задание

Построить модель угроз ИСПДн Вашего предприятия. Для построения модели угроз необходимо проработать теоретический материал лабораторной работы и заполнить таблицы 2 и 3.

Таблица 2 – Характеристики для определения исходного уровня защищѐнности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	***Уровень защищенности***		
	Высокий	***Средний***	***Низкий***
По территориальному размещению			
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом			
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка)			
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации			
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;			
локальная ИСПДн, развернутая в пределах одного здания			
По наличию соединения с сетями общего пользования			
ИСПДн, имеющая многоточечный выход в сеть			
общего пользования;			
ИСПДн, имеющая одноточечный выход в сеть общего пользования;			
ИСПДн, физически отделенная от сети общего пользования			
По встроенным (легальным) операциям с записями баз персональных данных			
чтение, поиск;			
запись, удаление, сортировка;			
модификация, передача			
По разграничению доступа к персональным данным			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;			
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;			
ИСПДн с открытым доступом			
По наличию соединений с другими базами ПДн иных ИСПДн			

интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);			
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн			

По уровню обобщения (обезличивания) ПДн

ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области,			

Технические и эксплуатационные характеристики ИСПДн	***Уровень защищенности***		
	Высокий	***Средний***	***Низкий***
региона и т.д.);			
~~ИСПДн, в которой данные обезличиваются~~ только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;			
~~ИСПДн, в которой предоставляемые~~ пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн			
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн ~~без предварительной обработки~~			
ИСПДн, предоставляющая всю базу данных с ПДн			
ИСПДн, предоставляющая часть ПДн			
ИСПДн, не предоставляющая никакой ~~информации~~			
Количество баллов по уровням			
Процент характеристик ИСПДн по уровням			
Уровень исходной защищѐнности ИСПДн			
Коэффициент защищѐнности ИСПДн (Y_1)			

Таблица 2 – Модель угроз ИСПДн «предприятия»

Угрозы безопасности ПДн	Вероятность реализации угрозы	Показатель опасности угрозы для ИСПДн	Возможность реализации угрозы	Актуальность угрозы	Примечание
Угрозы утечки информации по техническим каналам					
Угрозы утечки акустической информации					
Использование направленных(ненаправленных) микрофонов воздушной проводимости для съема акустического излучения информативного речевого сигнала					
использование "контактных микрофонов" для съема виброакустических сигналов					
использование "лазерных микрофонов" для съема виброакустических сигналов					
использование средств ВЧ-навязывания для съема электрических сигналов, возникающих за счет "микрофонного эффекта" в ТС обработки ПДн и ВТСС (распространяются по проводам и линиям, выходящим за пределы служебных помещений)					
применение средств ВЧ-облучения для съема радиоизлучения, модулированного информативным сигналом, возникающего при непосредственном облучении ТС обработки ПДн и ВТСС ВЧ-сигналом					
применение акустооптических модуляторов на базе ВОЛ, находящихся в поле акустического сигнала ("оптических микрофонов")					

Таблица 2 – Модель угроз ИСПДн «предприятия» (продолжение)

Угрозы безопасности ПДн	Вероятность реализации угрозы	Показатель опасности угрозы для ИСПДн	Возможность реализации угрозы	Актуальность угрозы	Примечание
Угрозы утечки видовой информации					
визуальный просмотр на экранах дисплеев и других средств отображения СВТ, ИВК, входящих в состав ИСПДн					
визуальный просмотр с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения СВТ, ИВК, входящих в состав ИСПДн					
использование специальных электронных устройств съема видовой информации (видеозакладки)					
Угрозы утечки информации по каналам ПЭМИН					
применение специальных средств регистрации ПЭМИН, от ТС и линий передачи информации (ПАК, сканерные приемники, цифровые анализаторы спектра, селективные микровольтметры)					

Таблица 2 – Модель угроз ИСПДн «предприятия» (продолжение)

Угрозы безопасности ПДн	Вероятность реализации угрозы	Показатель опасности угрозы для ИСПДн	Возможность реализации угрозы	Актуальность угрозы	Примечание
применение токосъемников для регистрации наводок информативного сигналов, обрабатываемых ТС, на цепи электропитания и линии связи, выходящие за пределы служебных помещений					
применение специальных средств регистрации радиоизлучений, модулированных информативным сигналом, возникающих при работе различных генераторов, входящих в состав ТС ИСПДн или при наличии паразитной генерации в узлах ТС					
применение специальных средств регистрации радиоизлучений, формируемых в результате ВЧ-облучения ТС ИСПДн в которых проводится обработка информативных сигналов -параметрических каналов утечки					

Таблица 2 – Модель угроз ИСПДн «предприятия» (продолжение)

Угрозы безопасности ПДн	Вероятность реализации угрозы	Показатель опасности угрозы для ИСПДн	Возможность реализации угрозы	Актуальность угрозы	Примечание
Угрозы НСД в ИСПДн					
Угрозы использования уязвимостей ИСПДн					
ошибки либо преднамеренное внесение уязвимостей при проектировании и разработке СПО и ТС, недекларированные возможности СПО					
ошибки либо преднамеренное внесение уязвимостей при проектировании и разработке ППО, недекларированные возможности ППО					
неверные настройки ПО, изменение режимов работы ТС и ПО (случайное либо преднамеренное)					
сбои в работе ТС и ПО (сбои в электропитании, выход из строя аппаратных элементов, внешние воздействия электромагнитных полей)					
Угрозы непосредственного доступа в операционную среду ИСПДн:					
доступ к информации и командам, хранящимся в BIOS с возможностью перехвата управления загрузкой ОС и получения прав доверенного пользователя на АРМ					

Таблица 2 – Модель угроз ИСПДн «предприятия» (продолжение)

Угрозы безопасности ПДн	Вероятность реализации угрозы	Показатель опасности угрозы для ИСПДн	Возможность реализации угрозы	Актуальность угрозы	Примечание
доступ в операционную среду (локальную ОС отдельного ТС ИСПДн) с возможностью выполнения НСД вызовом штатных процедур или запуска специально разработанных программ					
доступ в среду функционирования прикладных программ (локальная СУБД, например)					
доступ непосредственно к информации пользователя, обусловленных возможностью нарушения ее конфиденциальности, целостности, доступности					
Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия					
сканирование сети и анализ сетевого трафика для изучения логики работы ИСПДн, выявления протоколов, портов, перехвата служебных данных (в том числе, идентификаторов и паролей), их подмены					
применение специальных программ для выявления пароля (сниффинг, IP-спуффинг, разные виды перебора)					
подмена доверенного объекта сети с присвоением его прав доступа, внедрение ложного объекта сети					
реализация угрозы отказа в обслуживании					

Таблица 2 – Модель угроз ИСПДн «предприятия» (продолжение)

Угрозы безопасности ПДн	Вероятность реализации угрозы	Показатель опасности угрозы для ИСПДн	Возможность реализации угрозы	Актуальность угрозы	Примечание
внедрение специализированных троянов, вредоносных программ					
сетевые атаки					
применение утилит администрирования сети					
подключение к ТС и системам					
Угрозы программно-математических воздействий:					
внедрение программных закладок					
внедрение вредоносных программ (случайное или преднамеренное, по каналам связи)					
внедрение вредоносных программ (случайное или преднамеренное, непосредственное)					
Угрозы несанкционированного физического доступа к съемным носителям информации					
повреждение носителя информации					
утрата носителя информации					
хищение носителя информации					
Угрозы доступа к ТС и системам обеспечения					
нарушение функционирования кабельных линий связи, оборудования					
нарушение функционирования ТС обработки информации, НЖМД					

Таблица 2 – Модель угроз ИСПДн «предприятия» (продолжение)

Угрозы безопасности ПДн	Вероятность реализации угрозы	Показатель опасности угрозы для ИСПДн	Возможность реализации угрозы	Актуальность угрозы	Примечание
доступ к системам обеспечения, их повреждение					
доступ к снятым с эксплуатации носителям информации (содержащим остаточные данные)					
Угрозы неправомерных действий со стороны лиц, имеющих право доступа к информации					
Несанкционированное изменение информации					
Несанкционированное копирование информации					
Угрозы разглашения информации					
разглашение информации лицам, не имеющим права доступа к ней					
передача защищаемой информации по открытым каналам связи					
копирование информации на незарегистрированный носитель информации, в том числе печать					
передача носителя информации лицу, не имеющему права доступа к имеющейся на нем информации					

Контрольные вопросы

Какие показатели необходимо рассчитать для построения модели угроз ПДн?
Что обозначает коэффициент реализуемости угрозы?
Какие угрозы являются актуальными?
В соответствии с каким нормативным документом строится модель угроз?
В соответствии с каким нормативным документом, и в каких случаях строится модель нарушителя?

Лабораторная работа 6.
Изучение действующей нормативной документации объекта информатизации

Цель работы: изучить действующую нормативную документацию объекта информатизации.

Теоретическая часть

Основным документом, регламентирующим безопасность объекта информатизации, является политика информационной безопасности.

Политика информационной безопасности – это совокупность правил, процедур, практических методов и руководящих принципов в области ИБ, используемых организацией в своей деятельности.

Прежде всего политика необходима для того, чтобы донести цели и задачи информационной безопасности компании. Необходимо понимать, что безопасник это не только инструмент для расследования фактов утечек данных, но и помощник в минимизации рисков компании, а следовательно — в повышении прибыльности компании.

Согласно отечественному стандарту ГОСТ Р ИСО/МЭК 17799-2005, политика информационной безопасности должна устанавливать ответственность руководства, а также излагать подход организации к управлению информационной безопасностью. В соответствии с указанным стандартом, необходимо, чтобы политика информационной безопасности предприятия как минимум включала:

определение информационной безопасности, еѐ общих целей и сферы действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации

изложение целей и принципов информационной безопасности, сформулированных руководством

краткое изложение наиболее существенных для организации

политик безопасности, принципов, правил и требований, например, таких как :

соответствие законодательным требованиям и договорным обязательствам ;

− требования в отношении обучения вопросам безопасности;

предотвращение появления и обнаружение вирусов и другого вредоносного программного обеспечения;

управление непрерывностью бизнеса;

− ответственность за нарушения политики безопасности.

определение общих и конкретных обязанностей сотрудников в рамках управления информационной безопасностью, включая информирование об инцидентах нарушения информационной безопасности

ссылки на документы, дополняющие политику информационной безопасности, например, более детальные политики и процедуры для конкретных информационных систем, а также правила безопасности, которым должны следовать пользователи.

Политика информационной безопасности компании должна быть утверждена руководством, издана и доведена до сведения всех сотрудников в доступной и понятной форме.

Для того чтобы политика информационной безопасности не оставалась только «на бумаге» необходимо, чтобы она была:

непротиворечивой – разные документы не должны по разному описывать подходы к одному и тому же процессу обработки информации

не запрещала необходимые действия – в таком случае неизбежные массовые нарушения приведут к дискредитации политики информационной безопасности среди пользователей

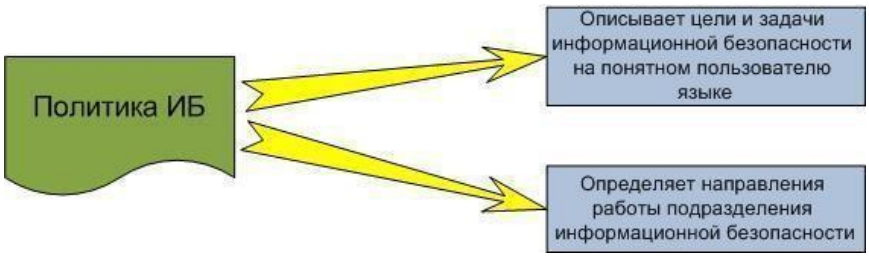
не налагала невыполнимых обязанностей и требований.

В организации должно быть назначено лицо, ответственное за политику безопасности, отвечающее за еѐ эффективную реализацию и регулярный пересмотр.

При разработке политики следует помнить о двух моментах.

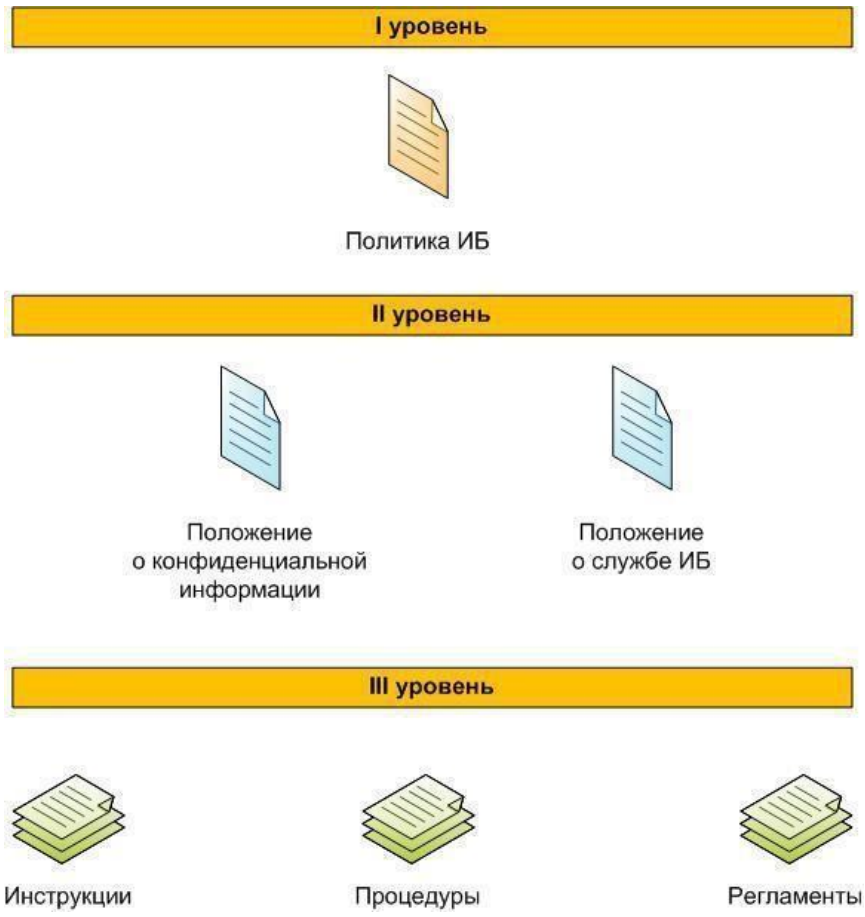
Целевая аудитория политики ИБ — конечные пользователи и топ-

менеджмент компании, которые не понимают сложных технических выражений , однако должны быть ознакомлены с положениями политики.
Не нужно пытаться включить в этот документ все, что можно. Здесь должны быть только цели ИБ, методы их достижения и ответственность!
Никаких технических подробностей, если они требуют специфических знаний. Это все — материалы для инструкций и регламентов.



Конечный документ должен удовлетворять следующим требованиям:

лаконичность — большой объем документа отпугнет любого пользователя, ваш документ никто никогда не прочитает (а вы не раз будете
употреблять фразу: «это нарушение политики информационной безопасности , с которой вас ознакомили»)
доступность простому обывателю — конечный пользователь должен понимать, ЧТО написано в политике (он никогда не прочитает и не запомнит слова и словосочетания «журналирование», «модель нарушителя», «инцидент информационной безопасности», «информационная инфраструктура », «техногенный», «антропогенный», «риск-фактор» и т.п.).
Политика ИБ должна быть документом первого уровня, ее должны расширять и дополнять другие документы (положения и инструкции), которые уже будут описывать что-то конкретное. Примерная схема представлена на рисунке.



Рассмотрим пример политики безопасности ОАО «Газпромбанк» — www.gazprombank.ru/upload/iblock/ee7/infibez.pdf. Имеется во вложении. На втором уровне рассматриваются положения о защищаемой информации и о отделе информационной безопасности в организации.

Пример положения о конфиденциальной информации находится во вложении.

Законы, регулирующие порядок работы с конфиденциальной информацией:

Федеральный закон "О защите персональных данных"

Федеральный закон О персональных данных. Данный закон, в частности, определяет требования к информационным системам персональных данных и регламентирует необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним.

Закон об архивном деле Федеральный закон Об архивном деле. Этот закон регулирует

отношения в сфере организации хранения, комплектования, учета и использования документов Архивного фонда Российской Федерации и других архивных документов независимо от их форм собственности.

Федеральный закон "О коммерческой тайне"

Федеральный закон о коммерческой тайне. Этот закон регулирует отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности.

Закон HIPAA

(Health Insurance Portability and Accountability Act of 1996) гласит, что:

«Все медицинские, страховые и финансовые организации, работающие с чувствительной медицинской информацией должны хранить не менее 6 лет всю свою электронную документацию».

Федеральный закон "О связи".

Настоящий Федеральный закон устанавливает правовые основы деятельности в области связи на территории Российской Федерации и на находящихся под юрисдикцией Российской Федерации территориях, определяет полномочия органов государственной власти в области связи, а также права и обязанности лиц, участвующих в указанной деятельности или пользующихся услугами связи.

Доктрина информационной безопасности.

Данный документ — совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ. Доктрина служит основой для: • формирования государственной политики в области обеспечения ИБ РФ; • подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения ИБ РФ; • разработки целевых программ обеспечения ИБ РФ. Доктрина ИБ РФ была утверждена 9.09.2000 года Президентом Российской Федерации В.В. Путиным.

Федеральный закон "Об информации, информационных технологиях и о защите информации".

Закон «Об информации, информационных технологиях и защите информации» определяет и закрепляет права на защиту информации и информационную безопасность граждан и организаций в ЭВМ и в информационных системах, а также вопросы информационной безопасности граждан, организаций, общества и государства. В законе дано правовое определение понятия «информация»: «информация — сведения (сообщения, данные) независимо от формы их представления».

Федеральный закон "Об электронной цифровой подписи"

В Законе РФ от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» прописаны условия использования ЭЦП, особенности еѐ использования в сферах государственного управления и в корпоративной информационной системе. Благодаря ЭЦП теперь, в частности, многие российские компании осуществляют свою торгово-закупочную деятельность в Интернете, через «Системы электронной торговли», обмениваясь с

контрагентами необходимыми документами в электронном виде, подписанными ЭЦП. Это значительно упрощает и ускоряет проведение конкурсных торговых процедур.

На третьем уровне рассматриваются инструкции, процедуры, регламенты.

Примеры документов:

- Инструкция по защите информации от компьютерных вирусов
- Инструкция по использованию электронной почты
- Инструкция по организации антивирусной защиты

Инструкция по эксплуатации компьютеров и работе в информационной сети

- Инструкция по организации парольной защиты

Инструкция по организации безопасной работы с информационной системой и копировальным оборудованием

Типовой регламент резервного копирования данных

Практическое задание

Составить перечень внутренних нормативных документов предприятия регламентирующих защиту информацию.

Провести сравнение имеющегося перечня нормативных документов с необходимым.

Написать один из внутренних документов, которые отсутствует на объекте информатизации.

Контрольные вопросы

Назовите структуру нормативных документов предприятия.
Какой документ по защите информации является первичным нормативным актом на предприятии?
Перечислите законы, регулирующие порядок работы с конфиденциальной информацией.
Что регулирует закон об архивном деле?
Что регулирует Федеральный закон "О защите персональных данных"?
Что регулирует Федеральный закон "О коммерческой тайне"?
Что регулирует Федеральный закон "О связи"?
Перечислите общий список внутренних нормативных документов, которые должны быть на любом объекте информатизации?

Лабораторная работа 7.
Составление плана мероприятий по улучшению защищѐнности объекта информатизации

Цель работы: изучить методику составления плана мероприятий по улучшению защищѐнности объекта информатизации.

Теоретическая часть

Объект информатизации - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

На рынке защиты информации предлагается много отдельных инженерно-технических, программно-аппаратных, криптографических средств защиты информации. В литературе по защите информации можно найти описание методов и средств на их основе, теоретических моделей защиты. Однако для того, чтобы создать на предприятии условия эффективной защиты информации, необходимо объединить отдельные средства защиты в систему. При этом надо помнить, что главным элементом этой системы является человек. Причем человек является ключевым элементом системы и вместе с тем самым трудно формализуемым и потенциально слабым ее звеном.

Создание системы защиты информации (СЗИ) не является главной задачей предприятия, как, например, производство продукции и получение прибыли. Поэтому создаваемая СЗИ не должна приводить к ощутимым трудностям в работе предприятия, а создание СЗИ должно быть экономически оправданным. Тем не менее она должна обеспечивать защиту важных информационных ресурсов предприятия от всех реальных угроз.

План защиты информации решается достаточно эффективно применением в основном организационных мер. К ним относятся: режимные мероприятия, охрана, сигнализация и простейшие программные средства защиты информации

Главная цель создания СЗИ — достижение максимальной эффективности защиты за счет одновременного использования всех необходимых ресурсов, методов и средств, исключающих несанкционированный доступ к защищаемой информации и обеспечивающих физическую сохранность ее носителей.

Организация — это совокупность элементов (людей, органов, подразделений) объединенных для достижения какой-либо цели, решения какой-либо задачи на основе разделения труда, распределения обязанностей и иерархической структуры.

СЗИ относится к системам организационно-технологического (социотехнического) типа, т. к. общую организацию защиты и решение значительной части задач осуществляют люди (организационная составляющая), а защита информации осуществляется параллельно с технологическим процессами ее обработки (технологическая составляющая).

Серьезным побудительным мотивом к проведению перспективных исследований в области защиты информации послужили те постоянно нарастающие количественные и качественные изменения в сфере информатизации, которые имели место в последнее время и которые, безусловно, должны быть учтены в концепциях защиты, информации.

Организация защиты информации

С приемлемой степенью точности классифицируем информацию по важности для последующего выбора средств защиты и определения прав доступа. За точку отсчета, к примеру, можно принять требования закона РФ "О персональных данных", выполнение которых он обязывает практически все компании. Это позволяет определить относительную важность всей

информации и, впоследствии, определить необходимые средства для ее защиты, обеспечивающие не только требования закона, но и противодействие интересам последних групп потенциальных и реальных пользователей.

Выявляем доступность информации, подлежащей защите, перечисленным группам пользователей, при этом заметим, что каждая из групп, и, прежде всего, сотрудники, не должны иметь полный доступ ко всей информации. Необходимо определить их права по доступу к информации, построив своеобразную матрицу "информация-права_доступа" или "информация-группы_пользователи" и определить и разграничить полномочия, пока на бумаге.

Перечисленные ранее действия вполне по силам заинтересованным сотрудникам предприятия, имеющим соответствующие полномочия, но, поскольку они не являются специалистами в сфере защиты информации и информационной безопасности, остаются исключения:

настройка конфигураций программно-технических средств обеспечивает их функционирование и не отвечает требованиям безопасности;

традиционная (исторически сложившаяся) архитектура сети, как правило, не обеспечивает необходимую защиту информационных ресурсов и технологий их обработки;

нельзя проверять самого себя - решения сотрудников могут содержать ошибки;

технический персонал не владеет полной информацией о степени важности различных данных;

технический персонал не может оценивать целесообразность принятых административных решений.

Следующий шаг - увязываем полученные данные. Начнем с программно-технических средств. Убеждаемся, что параметры операционных систем (ОС) рабочих станций, как правило и к сожалению, соответствуют настройке

поставщика ОС, а все изменения, если и производились, были сделаны с единственной целью обеспечения требуемого функционирования. То же самое относится и к штатным службам и прочим сервисам, в том числе и действующим на серверах предприятия, что недопустимо. К примеру, пароли поставщиков оборудования, оставленные по умолчанию - частая причина дискредитации систем аутентификации и авторизации, предоставляющая полный доступ с максимальными правами любому желающему в самых защищенных системах. Отключение бездействующих и ненужных служб, как одного из требований повышения защищенности систем, без точных знаний их назначения может привести к непредсказуемым последствиям - от переустановки операционных систем до потери данных. Настройки телекоммуникационного оборудования не менее важны, т.к. неверно сконфигурированные профили и функции также могут привести к перехвату управления. Эти обстоятельства диктуют новые условия продолжения работы, а дальнейшие шаги требуют привлечения специалистов для согласованной работы по защите информации. Придется обратиться к специализированной компании для выполнения комплекса работ, перечисленных в предыдущем абзаце. Преимущества такого выбора описаны и хорошо известны. Приведем основные - персонал привлеченной компании обладает штатом экспертов с уникальным объемом знаний и практическим опытом в смежных областях ИТ-сферы:

информационная безопасность и защита информации, в т.ч. моделирование процессов, анализ рисков и угроз;

- архитектура телекоммуникационных сетей;
- операционные системы и штатные сервисы;
- прикладное программное обеспечение, приложения;
- защитное программное обеспечение;
- технические программные средства защиты информации;
- прочие ИТ-технологии и средства.

Итак, исключительные обстоятельства преодолены, часть специфических функций возложена на провайдера информационной безопасности, в частности, предложения по применению и выбор технических средств защиты информации при реальной необходимости. Настраиваем программно-технические средства по предоставленным рекомендациям, приводим в соответствие архитектуру корпоративной системы, внедряем политику парольной защиты, разделяем и/или изолируем независимые информационные и бизнес-процессы, внедряем разграничение прав доступа к информационным ресурсам. Попутно выясняем потрясающие скрытые штатные возможности наличных программно-технических средств - журналы регистрации системных событий, функции текущего аудита, системы обнаружения и предупреждения вторжений, защитное ПО, возможности шифрованного хранения и передачи данных, возможности перераспределения нагрузки, контентной фильтрации, управления внутренним и внешним трафиком и многое другое. Задействуем все необходимое для построения "эшелонированной" обороны от "условного" противника.

Достигнутое впечатляет, но только неискушенных. Сам человек, как источник сведений и их основной потребитель пока остается в стороне, а "человеческий" фактор — наиболее частая причина утечки или потери информации, т.е. безопасность предприятия определяется и мерой ответственности работника за действия, которые он совершает, и без внедрения или детализации формальных отношений поставленная цель останется по-прежнему не близкой.

Принимаемся за разработку и внедрение организационно-административных мер, регулирующих правила работы с информационными ресурсами и действия персонала в нештатных ситуациях. Масштаб работы, глубина проработки и формализации процессов и конечное количество документов определяются

совместной работой группы ответственного управленческого персонала предприятия и специалистами привлеченной компании. Придется пролистать и заметно "освежить" трудовые контракты, должностные инструкции и действующие на предприятии инструкции на предмет определения зон ответственности и соглашений о конфиденциальности, определить перечень необходимых инструкций и правил работы с программными и техническими средствами, регламенты резервного копирования, определить методы доступа к информационным ресурсам, в частности, разработать политику парольной защиты, предусмотреть, наконец, правила действия сотрудников в нештатных ситуациях.

Следует предусмотреть и способ доведения разработанных документов до персонала компании. Например, постоянное представление на внутреннем корпоративном web-сайте компании при обязательном подписании отдельных документов ответственными работниками, тогда любые, даже неумышленные, нарушения безопасности будут иметь конкретных авторов.

Естественно, перечень и состав каждого документа для каждого предприятия уникальны и нередко отличаются для разных подразделений одного предприятия, но при этом соответствуют единой политике информационной безопасности, целесообразность разработки которой тоже определяется на текущем шаге. Во избежание возможных коллизий с действующим законодательством содержание документов и их легализацию следует согласовать с юридической службой, если она есть на предприятии или воспользоваться услугами имеющего такой опыт провайдера ИБ.

Как удостовериться, что при разработке и внедрении мер ничто не забыто и не допущены ошибки? Придется предусмотреть метод и средства анализа защищенности ресурсов, определить интервалы и назначить ответственных среди штатного персонала за проведение

систематического контроля созданной системы ИБ. Для анализа программно-технических средств можно применить программные сканеры безопасности и внедрить их в корпоративную систему, а разработанную нормативную документацию приводить в соответствие при изменениях характера и состава бизнес-процессов, изменениях архитектуры сети и, с другой стороны, регулярно подвергать созданную систему защиты информации анализу на соответствие требованиям документации, т.е. проводить регулярный внутренний аудит.

Внедрение разработанных мер займет некоторое время, как и подготовка персонала, прежде, чем защита информации будет обеспечена на должном уровне. Но есть еще несколько вопросов, от решения которых будет зависеть достигнутый уровень защиты информации. Во-первых, развитие технологий, в том числе и используемых злоумышленниками, постоянный процесс, требующий и совершенствование средств защиты, а, во-вторых, кто гарантирует, что при внедрении даже незначительных изменений и последующей эксплуатации корпоративной информационной системы в ней не появятся новые уязвимости? Увы, но, в отличие от развитых стран, в нашей стране практика страхования информационных рисков пока еще отсутствует. И, наконец, разве можно качественно проверить самого себя? Ответ очевидный - единственное решение в проведении периодического внешнего аудита для подтверждения и поддержания заданного уровня защищенности, т.к. появление "слабого" звена в построенной системе приведет к ослаблению системы в целом. Регламенти регулярность проведения внешнего аудита могут быть определены в

процессе разработки организационных мер и закреплены в соответствующих распорядительных документах.

Следует заметить, что предложенная последовательность действий - фактическая квинтэссенция нашего опыта по организации информационной безопасности предприятий с различными формами собственности, разных сфер деятельности и разной величины - от нескольких рабочих мест в одном помещении до территориально распределенной структуры с полуторатысячным коллективом. Деньги считают все одинаково.

Безусловно, подобный подход имеет некоторые недостатки с точки зрения построения комплексной системы управления информационной безопасностью, но это уже другая задача, а преимущества рассмотренного решения очевидны:

достигнута поставленная цель - конфиденциальная информация защищена ;

значительная часть работ выполнена штатным заинтересованным персоналом;

- документировано текущее состояние информационной системы

предприятия;

предложенный подход позволил избежать неоправданной бюрократической волокиты с распределением обязанностей при выполнении работ ;

- предельно снижены затраты на достижение цели;

создана логически увязанная система защиты информации;

- создана база для построения системы информационной безопасности;
- существенно повышен уровень экономической безопасности предприятия.

Следует оценить и следующий факт - при настройке программно-технических средств использованы передовые методики и

рекомендации, разработанные различными отечественными и зарубежными ведомствами, специализированными в сфере защиты информации и информационной безопасности, в том числе и военизированными.

Практическое задание

Составить план мероприятий по улучшению информационной безопасности предприятия выбранного в лабораторной работе 1.

Контрольные вопросы

Дайте определение объекта информатизации.

Какая главная цель создания СЗИ?

Назовите последовательность шагов для улучшения защищенности объекта информатизации.

Какие исходные данные используются для составления плана по улучшению защищѐнности объекта информатизации?

Какими документами должен руководствоваться специалист по защите информации при составлении плана мероприятий по улучшению защищѐнности объекта информатизации?

Лабораторная работа 8.
Разработка политики информационной безопасности

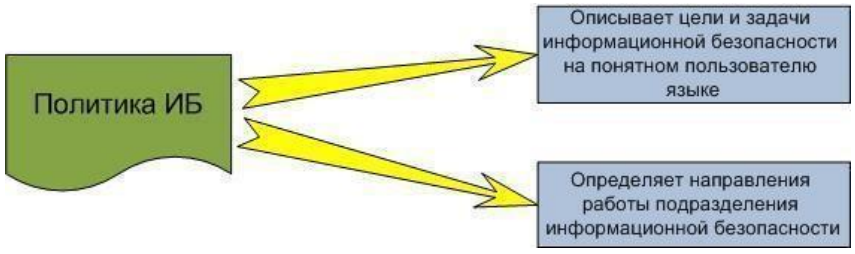
Цель работы: изучить структуру типовой политики информационной безопасности и научиться составлять частную политику информационной безопасности.

Теоретическая часть

Политика безопасности (информации в организации) (Organizational security policy) – это совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

В современной практике термин «политика безопасности» может употребляться как в широком, так и в узком смысле слова. В широком смысле политика безопасности определяется как система документированных управленческих решений по обеспечению безопасности организации. В узком смысле под политикой безопасности обычно понимают локальный нормативный документ, определяющий требования безопасности, систему мер, либо порядок действий, а также ответственность сотрудников организации и механизмы контроля для определенной области обеспечения безопасности.

Рисунок 1 – Задачи политики информационной безопасности



Примерами таких документов могут служить:
− Правила работы пользователей в корпоративной сети;
Политика обеспечения безопасности удаленного доступа к ресурсам корпоративной сети;
Политика обеспечения безопасности при взаимодействии с сетью Интернет ;
− Антивирусная политика, инструкция по защите от компьютерных вирусов ;
− Политика выбора и использования паролей;
− Правила предоставления доступа к ресурсам корпоративной сети;
− Политика установки обновлений программного обеспечения;
− Политика и регламент резервного копирования и восстановления данных;
− Соглашение о соблюдении режима информационной безопасности, заключаемое со сторонними организациями.
Разработка политик безопасности собственными силами – длительный трудоемкий процесс, требующего высокого профессионализма, отличного знания нормативной базы в области информационной безопасности. Поэтому решение вопроса о разработке эффективной политики информационной безопасности на современном предприятии обязательно связано с проблемой выбора критериев и показателей защищенности, а также эффективности корпоративной системы защиты информации. Вследствие этого, в дополнение к требованиям и рекомендациям стандартов, законам и иным руководящим документам приходится использовать ряд международных рекомендаций. В том числе адаптировать к отечественным условиям и применять на практике методики международных стандартов, таких как: ISO 17799, ISO 9001, ISO 15408, BSI, COBIT, ITIL и другие, а также использовать методики управления информационными рисками в совокупности с оценками экономической эффективности инвестиций в обеспечение защиты информации предприятия.

Основными нормативными документами в области информационной безопасности выступают:

«Общие критерии оценки безопасности информационных технологий» (ISO 15408),которые определяют функциональные требования безопасности и требования адекватности реализации функций безопасности;

«Практические правила управления информационной безопасностью» (ISO 17799). Данный стандарт содержит систему практических правил по управлению информационной безопасностью и используется в качестве критериев оценки эффективности механизмов безопасности на организационном уровне, включая административные, процедурные и физические меры защиты.

Для того чтобы сформировать и определить политику информационной безопасности, понадобятся следующие исходные данные:

Необходимо определить информацию, которая подлежит защите, и создать перечень сведений конфиденциального характера, в соответствии с защищаемой информацией;

Определить топологии средств автоматизации (физической и логической);

Необходимо описать административную структуру и категории зарегистрированных пользователей, описать технологию обработки информации и выделить потенциальных субъектов и объектов доступа;

− Определить угрозы безопасности информации и создать модель нарушителя ;
− Обнаружить и описать известные угроз и уязвимости;
− Расположить угрозы по убыванию уровня риска (провести анализ рисков).

Так же, необходимо описать общую характеристику и специализацию организации (наименование организации, специализация, род деятельности, решаемые задачи, характер и объем работ, расположение угроз по убыванию уровня риска).

Необходимо описать организационно-штатную структуру организации (отделы и отделения организации, наименования отделов, решаемые задачи, общая технологическая схема функционирования подразделений). Так же составляется общее описание рабочего процесса, технологическая схема операций при выполнении рабочего процесса, интенсивность, с которой выполняется рабочий процесс, технологические ограничения, средства контроля и критерии качества результатов рабочего процесса, перечень проблемных вопросов подразделений по обеспечению защиты информации.

Должны быть описаны так же следующие данные:

Используемые на предприятии средства вычислительной техники и программное обеспечение;

Сведения об используемых СВТ (описание аппаратных средств, коммуникационного оборудования удаленного доступа);

Сведения об используемом общем ПО (наименование и назначение, фирма разработчик, аппаратные требования, размещение);

Сведения об используемом специальном ПО (наименование и назначение, фирма разработчик, аппаратные требования, функциональные возможности , размещение).

Организация и структура информационных потоков и их взаимодействие :

− Топология ЛВС;

− Схема коммуникационных связей;
Структура и состав потоков данных (перечень входных информационных объектов и их источники, перечень выходных
информационных объектов и их получатели, перечень внутренних информационных объектов);
Организация хранения данных.
Общая характеристика автоматизированных систем организации: − Расположение ЛВС;
Технические и программные средства ЛВС (физическая среда передачи, используемые протоколы, операционные системы, серверы баз
данных, места хранения конфиденциальных данных, средства защиты информации);
Технические и программные средства доступа к ЛВС из сетей общего доступа;
− Принадлежность и типы каналов связи;
Сетевые протоколы удаленного доступа.

Ответственность и обязательства персонала

Эффективная информационная безопасность требует соответствующего участия персонала. Персонал ответственен за свои действия и, следовательно, отвечает за все события и последствия под своим идентификационным кодом пользователя (логин/пароль). Придерживаться политик и процедур доступа к сетям и системам – обязанность персонала.
Доступ к любым внешним Интернет-сервисам от имени компании равно как и доступ с помощью посторонних ИТ ресурсов к бизнесу компании не компенсируется, не существует без обязательств, ответственности и согласия компании.
Ответственность персонала включает, но не ограничивается следующим: считывать и передавать только данные, на которые у Вас есть авторизованные права и которые Вам положено знать, включая ошибочно адресованную электронную почту;
сознательно придерживаться всех политик, законов и нормативных

документов (локальных, федеральных, международных), касающихся использованию компьютерных систем и программ;
сообщать о нарушениях информационной безопасности ответственным за безопасность сотрудникам, тесно сотрудничать в
расследованиях злоупотреблений и неправомерных действий персонала с ИТ ресурсами ;
защищать назначенные Вам имя и коды пользователя, пароли, другие ключи доступа от раскрытия;
оберегать и содержать конфиденциальную печатную информацию, магнитные и электронные носители в предназначенных для этого местах, когда они не в работе и размещать их в соответствии с политикой компании;

использовать только приобретенное компанией и лицензионное программное обеспечение, разрешенное для использования внутри
компании, устанавливать программы и сервисы только через сотрудника ИТ подразделения;
выполнять все предписания и действия по информационной безопасности (например, по антивирусной защите, пользованию электронной
почтой); не оставлять компьютер с включенным доступом в свое отсутствие - ставить экран на пароль или выходить из системы;
не перегружать ресурсы компании (каналы и сервера) трафиком,
запуском нескольких копий программ; сворачивать или закрывать неиспользуемые программы на сервере;
периодически посещать тренинги и семинары, проводимые ИТ подразделением компании.

Политика разрешения доступа к технологическим ресурсам

Политика разрешения доступа к технологическим ресурсам подразделения, службы, отделы, чья деятельность связана с использованием ИТ ресурсов компании, выдачей разрешений доступа к этим ресурсам.

Описывает процедуры, которые должны быть выполнены всеми участниками процесса разрешения доступа к ИТ ресурсам компании.
Весь персонал, допущенный к работе с ИТ ресурсами компании, должен :
− иметь соответствующую компьютерную подготовку;

пройти тестовый контроль и, при необходимости, обучение работе с корпоративными информационными системами;
получить и иметь авторизованный доступ к выделенным ему ресурсам ;
− ознакомиться и соблюдать политики безопасности, установленные компании.
Службы по подбору персонала, руководители подразделений, отдел кадров, бухгалтерия и др. обязаны согласовывать любые действия по регламентированию, подбору, перемещению, увольнению вышеуказанного персонала с ИТ подразделением и его службой ИБ, строить свою работу с учетом настоящей политики.
ИТ подразделение обязано провести тестовый контроль каждого нового или перемещаемого сотрудника на возможность допуска к ИТ ресурсам компании, а в случае положительного решения провести следующие мероприятия по обеспечению доступа:
− ознакомить с политиками ИБ компании (под роспись);
разъяснить структуру, состав и организацию информационной системы в рамках должностных обязанностей нового сотрудника;
разъяснить пределы компьютерной самопомощи, после которой персонал может обращаться в службу поддержки HelpDesk (см. Политику информационно-технической поддержки);
выделить ему информационные ресурсы и пространство, наделить (зарегистрировать, авторизовать) его идентификационным(и) номером (ами), паролем (ями), правами согласно Политике паролей;
произвести настройки для пользования e-mail, Интернет и другими внешними ресурсами;

выдать имеющиеся инструкции, распоряжения, руководства, касающиеся его будущей работы с ИТ ресурсами;
у увольняемого сотрудника – принять ресурсы и дезактивировать его авторизацию.

Обслуживаемые ИТ подразделением технологические ресурсы должны быть настроены для аутентификации (идентификации и авторизации) конечных пользователей.
Обучение персонала работе с новыми приложениями может осуществляться с участием сторонних организаций.
При приеме на работу персонал должен быть инструктирован по вопросам режима в помещениях, хранения, обмена, подготовки бумажных/электронных документов, пользования факсом, междугородней и международной связью, а также по пожарной и электробезопасности.
К любому сотруднику, замеченному в нарушении этой политики, могут применяться дисциплинарные взыскания, вплоть до увольнения с работы.

Политика пользования электронной почтой

Политика пользования электронной почтой предоставляет персоналу разрешенные правила пользования ресурсами электронной почты (e-mail) компании. Политика охватывает e-mail, приходящий или отправляемый через все принадлежащие компании персональные компьютеры, сервера, ноутбуки, терминалы, карманные переносные компьютеры, сотовые телефоны и любые другие ресурсы, способные посылать или принимать e-mail по протоколам SMTP, POP3, IMAP.
Компании принадлежат все e-mail системы, в т.ч. используемые на правах аутсорсинга, сообщения сгенерированные и обработанные e-mail системами, включая архивные копии, и вся содержащаяся в них информация. Несмотря на то, что персонал получает индивидуальный пароль для доступа к e-mail системам, все они остаются собственностью компании.

Компания контролирует с/без предупреждения содержание e-mail для разрешения проблем, обеспечения безопасности и исследования активности. Сообразно с принятыми бизнес-практиками, компания собирает статистические данные о своих ИТ ресурсах. ИТ персонал компании контролирует использование e-mail, чтобы гарантировать текущую доступность и надежность систем.

Персонал может подвергаться лишению прав пользования e-mail и/или дисциплинарным взысканиям, вплоть до увольнения с работы, при выявлении действий, противоречащим настоящей политике.

Персонал должен сохранять конфиденциальность своих паролей и, независимо от обстоятельств, *никогда не передавать в пользование и не раскрывать их никому*.

Персонал должен использовать электронную почту компании для любой переписки, касающейся деятельности компании. Использование внешних почтовых сервисов (ящиков) допустимо только по согласованию со службой ИБ.

Персонал должен ограничивать объемы пересылаемой по e-mail информации, чтобы не перегружать и не блокировать каналы связи. Объем почтового сообщения с вложением не должен превышать 300Кбайт.

Пересылаемая текстовая информация должна сжиматься стандартными архиваторами. Пересылаемая графическая информация должна сжиматься стандартными средствами пакета Microsoft Office – Picture Manager.

Персонал должен готовить e-mail сообщения, соответствующие по виду и содержанию официальному имиджу компании.

Персонал должен удалять подозрительные сообщения и сообщения от незнакомых адресатов, при необходимости заботиться о ежедневном обновлении антивирусной базы.

Приветствуется использование технологии считывания только заголовков почтовых сообщений, что резко сокращает вирусную опасность и трафик, связанный со спамом.

Компания обеспечивает персонал e-mail системами для облегчения бизнес коммуникаций и поддержки ежедневных рабочих операций.

Этично и приемлемо

связываться и обмениваться информацией согласно с миссией, характером и рабочими задачами компании, использование личной переписки допустимо, но она должна храниться в отдельных папках;
использовать общепринятую лексику и ограничения в словесных описаниях , принятых в компании;
уважать легальную защиту, которую предусматривают различные права пользования и лицензии на ПО и данные;
придерживаться грамотного ведения e-mail, удалять устаревшие сообщения , в т.ч. с почтового сервера и т.д.

Запрещено и наказуемо

нарушать любые законы, политики компании или правила;

подавать, публиковать, показывать или передавать любую информацию или данные, содержащие клевету, ложь, неточности, оскорбления, непристойности, порнографию, богохульство, сексуальные домогательства, угрозы, расовые и национальные обиды и агрессивные
комментарии, дискриминацию по полу, цвету волос и пр. или неверный материал ;
нарушать приватность персонала, клиентов, данных и/или
использовать информацию, содержащуюся в компании, в личных интересах или выгоды;
заниматься рассылкой и пересылкой писем других лиц, распространением недозволенной и другой рекламы и пр.;
намеренное размножение, разработку или выполнение
вредоносного программного обеспечения в любых формах (вирусы, черви, трояны и пр.);
просмотр, перехват, раскрытие или помощь в просмотре, перехвате, раскрытии e-mail, не адресованной Вам.

Антивирусная политика

Антивирусная политика применяется ко всем компьютерам сети компании, каталогам общего пользования, к которым относятся настольные компьютеры, ноутбуки, file/ftp/proxy серверы, терминалы, любое сетевое оборудование, генерирующее трафик. Источниками вирусов могут быть e-mail, Интернет-сайты со скрытыми вредоносными активными элементами, носители информации (флоппи-диски, CD-диски, flash-диски и пр.), открытые для общего доступа папки и файлы и т.д.
Защита от внешних угроз и вирусов имеет несколько уровней: а) антивирусный контроль на почтовом сервере провайдера; б) защита от внешних вторжений, вирусов с Интернет-сайтов и трафика во вне с помощью ISA-серверов; в) антивирусный контроль файлов и почтовых вложений с

помощью антивирусных программ на серверах и рабочих станциях пользователей; г) анти-шпионские сканеры (дополнительно); д) персональные брэндмауэры (дополнительно).
На всех компьютерах сети должно быть установлено соответствующее стандартам компании антивирусное программное обеспечение, а в некоторых случаях в сочетании с персональным брэндмауэром. Антивирус « патрулирует» жесткий диск и память компьютера на проникновение вируса, а брэндмауэр контролирует данные, попадающие и покидающие «внутренний периметр» через Интернет-соединение.

Это программное обеспечение должно выполняться постоянно или настроено для регулярного исполнения по расписанию. Кроме того,
антивирусные базы должны обновляться в срок (автоматически или вручную). Инфицированные вирусами компьютеры должны удаляться из сети до полного уничтожения вирусов. Работы по уничтожению вирусов, обновлению антивирусных баз на сервере, настройке запуска антивирусных процедур по расписанию выполняются службой системного администрирования (СА).
Все сотрудники, допущенные к работе с информационно-технологическими ресурсами компании, должны владеть навыками работы с антивирусными инструментами. Антивирусное сканирование конечные пользователи выполняют самостоятельно.
Любая деятельность по намеренному созданию и/или распространению вредоносных программ внутри сети компании (вирусы, черви, трояны, почтовые бомбы и пр.) запрещена.
К любому сотруднику, замеченному в нарушении этой политики, могут применяться дисциплинарные взыскания, вплоть до увольнения с работы.

Рекомендованные антивирусные процедуры

всегда запускайте доступное на корпоративном сервере (сайте) антивирусное программное обеспечение. Скачивайте, запускайте и
устанавливайте текущие версии антивирусных обновлений по мере их доступности ;
НИКОГДА не открывайте вложенные (присоединенные) к e-mail файлы или макросы от неизвестных, подозрительных или недостоверных
источников. Удаляйте эти вложения немедленно, затем удаляйте их « физически» из корзины (папки) удаленных;
удаляйте и не пересылайте спам, рассылки и случайные e-mail сообщения ;
используйте технологии считывания только заголовков почтовых сообщений, что резко сокращает вирусную опасность и трафик, связанный со спамом ;
никогда не скачивайте файлы с неизвестных, подозрительных и « зазывающих» Интернет-сайтов;

избегайте предоставления дискового пространства для чтения /записи, кроме случаев абсолютной бизнес необходимости делать так;
всегда сканируйте на вирусы носители информации (флоппи-диски, CD -диски, flash-диски и пр.) от неизвестных источников;
при возникновении угроз, выявленных персональным брэндмауэром – контрольно-пропускным пунктом для всех Ваших данных –
НЕ разрешайте доступ неизвестным Вам приложениям; обращайтесь в службу СА;
свои критические данные и системные настройки периодически сохраняйте в безопасных местах: в локальной основной папке (Мои
документы), в резервной папке в другом разделе своего диска, на сервере, на flash -диске;
если антивирусная программа (защита) отключена, никогда не
запускайте приложения, которые могут передать вирус (например, e-mail, Internet explorer, общий доступ к файлам и пр.);

при конфликтах в сети, замедлении работы, зависании и других необычных проявлениях в работе компьютера, всегда «останавливайте», «закрывайте» все программы и запускайте сканирующие антивирусные программы для гарантированного лечения компьютера;
в дополнение к предыдущему пункту, хорошим тоном является визуальное наблюдение «Интернет и сетевой активности» компьютера в фоновом режиме с помощью (разрешенных в компании) программ, следящих

за каналом связи и индицирующим трафик на экране (типа DU Meter для рабочих станций);
новые вирусы появляются почти каждый день ... поэтому следует периодически пересматривать настоящую антивирусную политику и рекомендованные антивирусные процедуры.

Политика подготовки, обмена и хранения документов

Политика подготовки, обмена и хранения документов охватывает все подразделения, службы, отделы, чья деятельность связана с подготовкой, копированием, хранением, обменом документами, информацией, данными с использованием информационно-технологических ресурсов компании.
Персонал компании должен придерживаться следующих требований по подготовке, копированию, хранению, обмену документами, информацией, данными , файлами:
по содержанию:
документы по виду и содержанию должны соответствовать официальному имиджу компании, следует употреблять общепринятую деловую лексику;
следует избегать употребления слов и выражений, раскрывающих критическую деятельность компании, в необходимых случаях использовать сокращения .
по хранению электронных документов:

документы офисных, почтовых, графических и др. стандартных приложений (Word, Excel, PowerPoint, Outlook, PhotoShop и пр.) должны
создаваться и храниться в папках Мои Документы; все папки должны иметь понятную вложенную структуру и наименования по темам; личные файлы, не относящиеся к деятельности компании, должны храниться в отдельной папке;
критичные для компании документы после создания и обработки

следует хранить в общедоступной папке Для Обмена – на сервере, в личных подпапках ;
полный доступ к личной подпапке в Для Обмена на сервере имеет
владелец папки, доступ на чтение могут иметь другие пользователи согласно разрешениям доступа;
запрещено хранить личные файлы, не относящиеся к деятельности компании , на серверах компании;
периодически, раз в неделю удалять устаревшие версии файлов с сервера - из личных папок Для Обмена и Мои Документы;
корпоративные базы данных (Navision, 1C, Access и др.) должны
храниться на серверах компании, архивироваться по расписанию, иметь разграниченный авторизованный доступ для персонала;
копировать данные на внешние накопители типа CD/DVD-RW, USB FlashDrive, FlashCard и пр. разрешено лицам, имеющим особое разрешение.
по обмену электронными документами:

разрешено считывать, передавать, изменять только данные, на
которые у Вас есть авторизованные права и которые Вам положено знать, включая ошибочно доступные папки и электронную почту;
внутриофисный обмен файлами может выполняться через

общедоступную папку на сервере (ДляОбмена); внутриофисный обмен по электронной почте через Интернет ограничивается;
межофисный обмен файлами выполняется по электронной почте e-mail (см. Политику пользования электронной почтой); разрешено использовать интерактивный обмен сообщениями программами типа Messenger, ISQ;
− терминальная работа на удаленных серверах выполняется по VPN- каналу ;
− межофисный обмен данными между удаленными корпоративными базами осуществляется специальными средствами через Интернет, в архивированном виде, критичный трафик может шифроваться стандартными средствами .

по хранению бумажных документов:

− оберегать и содержать конфиденциальную печатную информацию, также магнитные и электронные носители, фирменные бланки, печати, штампы в предназначенных для этого контейнерах, полках, стеллажах, сейфах, когда они не в работе;
не держать бумажные документы на столе в пределах визуальной доступности во время отсутствия на рабочем месте, хранить в папках по темам ;
не делать лишних ксерокопий и печатных копий документов, не оставлять документы в неположенных местах; следует уничтожать ненужные критичные документы, в т.ч. с помощью уничтожителя бумаги.

по обмену бумажными документами:

электронный обмен документами предпочтительнее обмена бумажными документами;
бумажный документ следует передавать адресату в пределах офиса лично в руки, в другой офис – по регламенту через курьера.

Внутриофисный обмен и движение документов предпочтительнее организовать с помощью специальных программ документооборота и коллективной работы типа Exchange, Share Point и др.
К любому сотруднику, замеченному в нарушении этой политики, могут применяться дисциплинарные взыскания, вплоть до увольнения с работы.

Политика информационно-технической поддержки

Политика информационно-технической поддержки охватывает и описывает все уровни поддержки персонала, выполняемые *по заявкам* через службу **HelpDesk** - единой точки контакта с персоналом. Выделяется уровень самопомощи и три уровня поддержки:

Самопомощь – когда конечный пользователь самостоятельно выполняет действия по устранению проблемы, не нарушающие безопасности сети и других пользователей, такие как перезапуск приложения или компьютера, проверка подключения все кабелей и сетевых ресурсов, антивирусное сканирование и пр.

HelpDesk 1-го уровня – выполняет поддержку заявок ***общего профиля***:

решение оперативных проблем персонала, задач доступа и безопасности ;
первичная диагностика сложных проблем, причин не работы программ ;
устранение проблемы или переадресация по сложности на следующий уровень.

3. ***HelpDesk 2-го уровня*** – выполняет поддержку заявок по ***работе приложений и систем***:

– углубленные, содержательные консультации и обучение;
поиск решений имеющимися средствами (без вмешательства в логику приложений), помощь в выборке и восстановлении данных и документов , в бизнес анализе, (раз)доработка отчетных форм;
обслуживание контента и администрирование Интернет-сайта компании ;
формулирование задач для изменяющихся бизнес-процессов, составление нормативных документов.

4. ***HelpDesk 3-го уровня*** – выполняет поддержку заявок по ***развитию приложений, систем, инфраструктуры***:

− исследования, доработка, лабораторное тестирование, выработка решений ;

− работа с поставщиками приложений и разработчиками;

планирование и развертывание новых приложений, реорганизация процессов и пр..

Поддержка *HelpDesk* закрепляется по уровням за организационными единицами ИТ подразделения: службой СА и эксплуатации стандартных средств , службой ИБ, службой поддержки прикладных программ и систем.

Персонал должен обращаться в *HelpDesk 1-го уровня* только после выполнения разрешенных процедур самопомощи. Многократное обращение в *HelpDesk* по инцидентам, устраняемым самопомощью, указывает на несоответствие персонала занимаемой должности.

ИТ обслуживание персонала осуществляется **по заявкам**. Содержание заявки передается в ИТ подразделение **любым доступным способом** (телефон, почта, бумажный носитель). Заявка должна быть зарегистрирована в **журнале заявок** (инцидентов), конечный пользователь информирован о порядке, времени исполнения заявки, ее движении, и, по возможности, обеспечен альтернативными ресурсами. Приоритет исполнения заявки устанавливается в связи с текущими бизнес задачами компании, временны*ы*ми и кадровыми возможностями службы *HelpDesk.*

Результаты исполнения заявки также должны быть зафиксированы в журнале. Журнал (база данных) инцидентов должен вестись полно и аккуратно – он является неотъемлемой частью системы управления ИБ, управления инцидентами и проблемами, основой для выявления их причин и тенденций.

Совмещение функций приема заявок и функций разрешения инцидентов считается ошибочным и требует разделения.

Работы по *HelpDesk 3-го уровня* должны выполняться на проектной основе и, возможно, с привлечением внешних консультантов, подрядчиков. Внешние консультанты и подрядчики должны иметь максимально ограниченный доступ к информационно-техническим ресурсам компании, но достаточный для выполнения проектов. Для ведения проектов со стороны компании назначаются руководитель проекта, члены проектной команды.

К любому сотруднику, замеченному в нарушении этой политики, могут применяться дисциплинарные взыскания, вплоть до увольнения с работы.

Политика серверной безопасности

Политика серверной безопасности применяется к серверному оборудованию, принадлежащему и используемому в компании, и к серверам, зарегистрированным в принадлежащих компании внутренних сетевых доменах.
Все внутренние сервера, развернутые в компании, должны быть в ведении ИТ подразделения, а именно группы системного администрирования (СА). Группа СА должна установить и поддерживать правила разрешенных серверных конфигураций, основанных на потребностях бизнеса и утвержденных службой ИБ. Группа СА должна следить за соответствием конфигурации и проводить политику ограничения, наложенную на сетевое окружение. Группа СА должна также установить правила и процессы смены конфигураций, включающие проверку и разрешение службы ИБ.
Все серверы компании должны быть идентифицированы: а) имя и местонахождение; б) перечень и версии оборудования и операционной системы; в) главные функции и развернутые приложения. Изменения конфигураций и назначения серверов должны сопровождаться соответствующим изменением процедур управления.
Основы конфигурирования – правила
⁻серверная инфраструктура должна строиться на базе технологий

Windows 2003 Server – доменная структура, ActiveDirectory, терминальный доступ и пр.

конфигурация операционной системы должна быть настроена в соответствии с разрешениями службы ИБ;

неиспользуемые сервисы и приложения должны быть отключены (деактивированы);

доступ к сервисам должен протоколироваться и/или, если возможно , защищаться;

все последние заплатки, сервис-паки и процедуры безопасности должны быть установлены в системе сразу, как только это возможно;

исключением могут быть неотложные приложения, пересекающиеся с потребностями бизнеса;

доверительные отношения между системами есть риски ИБ и их

следует избегать; не следует использовать доверительные отношения, когда существуют другие методы связи, обмена;

¯всегда следует использовать стандартные принципы безопасности,

частности, принцип «минимального требуемого доступа» для выполнения функций;

не следует использовать корневые папки и базовые процедуры для

обслуживания непривилегированных учетных записей; доступ к ним должен быть закрыт;

удаленный доступ по VPN должен осуществляться по защищенным

каналам (например, шифрование с ключом или использование сертификатов);

серверы физически должны быть расположены в помещениях с необходимым климат- и доступ- контролем; категорически запрещена работа серверов в неконтролируемых, слишком малых помещениях;

критичное для компании серверное ПО должно резервироваться, создаваться образы; резервные сервера должны быть сконфигурированы аналогично основным, для быстрой замены основных серверов.

Мониторинг:

Выявление небезопасных событий серверной сетевой инфраструктуры

должно обеспечиваться средствами Windows 2003 Server и специализированными продуктами Microsoft. Небезопасные события включают , но не ограничиваются следующим:

- атака по сканированию портов;
- очевидный неавторизованный доступ к учетным записям;

аномальное поведение и инциденты, не свойственные конкретным приложениям на хосте.

Небезопасные события должны анализироваться и, в случае необходимости, предприниматься восстановительные и нейтрализующие мероприятия .

Соглашения:

аудит должен выполняться регулярно службой ИБ компании, согласно политике аудита;

служба ИБ отбирает и представляет в службу СА сведения для надлежащей поддержки, корректировки и настройки персонала;

физическая безопасность серверов находится в ведении службы охраны и безопасности компании;

− руководство компании ответственно за своевременное выделение средств на приобретение серверного оборудования, программного обеспечения, обучения специалистов компании.

К любому сотруднику, замеченному в нарушении этой политики, могут применяться дисциплинарные взыскания, вплоть до увольнения с работы.

Практическое задание

Написать политику безопасности для выбранного предприятия.

Контрольные вопросы

Дайте определение политики информационно безопасности.

Из каких основных документов состоит политика информационной безопасности?

Назовите общее содержание политики разрешения доступа к технологическим ресурсам.
Что включает в себя политика пользования электронной почтой?
Назовите общее содержание антивирусная политика.
Назовите общее содержание политика подготовки, обмена и хранения документов.

Что включает в себя политика информационно-технической поддержки?
Что включает в себя политика серверной безопасности?

Лабораторная работа 9.
Исследование методов выбора рационального варианта системы защиты информации на основе экспертной информации.

Цель работы: изучить метод экспертной оценки информации, изучить методы выбора рационального варианта системы защиты на основе экспертной информации.

Теоретическая часть

Анализ методов решения задачи выбора рационального варианта СЗИ

Принципиальными особенностями решения задачи выбора рационального варианта СЗИ, определяющими метод ее решения являются:

−многокритериальность задачи выбора;

не только количественное, но и качественное (нечеткое) описание показателей качества СЗИ, задаваемых в виде требований;

при нечеткой постановке задачи влияние на выбор метода ее решения экспертной информации, определяющей предпочтение того или иного показателя.

Рассмотрим указанные особенности решения задачи более подробно.

Общая постановка задачи многокритериальной оптимизации имеет следующий вид.

Пусть $X = | x1 ,..., xi ,..., xn |$ - вектор оптимизируемых параметров некоторой системы S. Некоторое j-е свойство системы S характеризуется величиной j-го показателя $qi\ (X\ )$; $j = 1, m$. Тогда система в целом характеризуется вектором показателей $Q = | q1,..., q\ j\ ,..., qm$. Задача многокритериальной оптимизации *сводится к тому, чтобы из множества M_s вариантов системы S выбрать такой вариант (систему S_0), который обладает наилучшим значением вектора Q .*

При этом предполагается, что понятие "наилучший вектор Q "

предварительно сформулировано математически, т.е. выбран (обоснован) соответствующий критерий предпочтения (отношение предпочтения).

Анализ литературы показывает, что все многочисленные методы решения многокритериальных задач можно свести к трем группам методов:

−метод главного показателя;

−метод результирующего показателя;

−лексикографические методы (методы последовательных уступок).

Метод главного показателя основан на переводе всех показателей качества, кроме какого-либо однородного, называемого главным, в разряд ограничений типа равенств и неравенств. Присвоим главному показателю номер $q_1(S)$. Тогда задача сводится к однокритериальной задаче выбора системы $S \in$ Ms , обладающей минимальным значением показателя $q1(S)$ при наличии ограничений типа равенств и неравенств, т.е. имеет вид:

$$\min_{S \in M_s} q_1(S) \qquad (1)$$

при ограничениях:

$$q_j(S) = q_{j0}; \quad J = 2,...,l;$$

$$q_k(S) \le q_{k0}; \quad k = l+1,..., p; \qquad (2)$$

$$q_r(S) \ge q_{r0}; \quad r = p+1,...,m;$$

Методу главного показателя присущи следующие недостатки:

1. В большинстве случаев нет достаточных оснований для того, чтобы считать какой-то один и притом вполне определенный показатель качества является главным, а все остальные – второстепенными.
2. Для показателей качества $q_2(S)$, ..., $q_m(S)$, переводимых в разряд ограничений, достаточно трудно установить их допустимые значения.

Метод результирующего показателя качества основан на формировании обобщенного показателя путем интуитивных оценок влияния

частных показателей качества $q_1, ..., q_m$ на результирующее качество выполнения системой ее функций. Оценки такого влияния даются группой специалистов – экспертов, имеющих опыт разработки подобных систем.

Наибольшее применение среди результирующих показателей качества получили аддитивный, мультипликативный и минимаксный показатели.

Аддитивный показатель качества представляет собой сумму взвешенных нормированных частных показателей и имеет вид:

$$Q = \sum_{j=1}^{m} \omega^j \overline{q^j} \qquad (3)$$

где $\overline{q^j}$ - нормированное значение j-го показателя;

ω^j -весовой коэффициент j-го показателя, имеющий тем большую величину, чем большее влияет на качество системы;

$$\sum_{j=1}^{m} \omega_j = 1; \omega_j > 0; j = \overline{1, m}$$

Главным недостатком аддитивного показателя является то, что при его применении может происходить взаимная компенсация частных показателей. Это значит, что уменьшение одного из показателей вплоть до нулевого значения может быть компенсировано возрастанием другого показателя. Для ослабления этого недостатка вводятся специальные ограничения на минимальные значения частных показателей, на их веса, а также используются другие приемы.

Мультипликативный показатель качества образуется путем перемножения частных показателей с учетом их весовых коэффициентов и имеет вид:

$$Q = \prod_{j=1}^{m} \overline{q_j}^{\omega_j} \qquad (4)$$

где $\overline{q_j}$ и ω_j имеет тот же смысл, что и в аддитивном показателе.

Наиболее существенное отличие мультипликативного показателя от аддитивного заключается в том, что аддитивный показатель базируется на

принципе справедливой абсолютной уступки по отдельным показателям, а мультипликативный — на принципе справедливой относительной уступки. Суть последнего заключается в том что справедливым считается такой компромисс, когда суммарный уровень относительного снижения одного или нескольких показателей не превышает суммарного уровня относительного увеличения остальных показателей.

Максиминный показатель. **В** ряде случаев вид результирующей целевой функции достаточно трудно обосновать или применить. В подобных случаях возможным простым путем решения задачи является применение максиминного показателя. Правило выбора оптимальной системы S_0 в этом случае имеет следующий вид:

$$\max_{S \in M_s} \min_{1 \le j \le m} \{q^1(S),...,q^j(S),...,q^m(S)\} \quad (5)$$

если весовые коэффициенты частных показателей отсутствуют:

$$\max_{S \in M^s} \min_{1 \le j \le m} \{q^{\varpi 1}(S^{\omega j}(S),...,q^{\omega m}(S),...,q^{\omega m}(S)\} \quad (6)$$

если весовые коэффициенты определены.

Максиминный показатель обеспечивает наилучшее (наибольшее) значение наихудшего (наименьшего) из частных показателей качества.

Лексикографический метод.

Предположим, что показатели упорядочены по важности, например, $q_1(S) > q_2(S) > ... > q_m(S)$.

Суть метода заключается в выделении сначала множества альтернатив с наилучшей оценкой по наиболее важному показателю. Если такая альтернатива единственная, то она считается наилучшей; если их несколько, то из их подмножества выделяются те, которые имеют лучшую оценку по второму показателю и т.д.

Как в классической, так и в нечеткой постановке выбор метода решения многокритериальной задачи определяется тем, в каком виде представлена

экспертная информация о предпочтении показателей или их важности. Поэтому в заключение этого раздела приведем таблицу, которая позволяет обоснованно выбирать метод нечеткой многокритериальной оптимизации в зависимости от экспертной информации о предпочтении показателей (таблице 1).

Таблица 1 – Выбор метода

Экспертная информация о степени предпочтения или важности показателей	*Метод решения многокритериальной задачи*
отсутствует	максимальный метод (5)
показатели упорядочены до важности	лексикографический метод
определены весовые коэффициенты показателей	1. адаптивный показатель (3) 2. мультипликативный показатель (4) 3. максиминный показатель (6)

Используя рекомендации по выбору метода решения, в дальнейшем рассмотрим ряд конкретных методов и примеров решения задачи многокритериальной оптимизации СЗИ в нечеткой постановке.

Выбор варианта СЗИ при равной важности требований

Пусть имеется множество из m вариантов построения СЗИ:

$A = \{a_1, ..., a_2, ..., a_m\}$

Для некоторого требования С (критерия оценки) может быть рассмотрено нечеткое множество:

$$C = \{\mu^c(a^1)/a^1; \mu^c(a^2)/a^2; ...; \mu^c(a^m)/a^m\} \quad (7)$$

где $\mu^c(a^i) \in [0,1]$ - оценка варианта a_i, по критерию С, которая характеризует степень соответствия варианта требованию определенному критерием С.

Если имеется n требований: $C^1, C^2, ..., C^n$, $j = 1, n$, то лучшим считается вариант, удовлетворяющий и требованию $C_1, C_2, ..., C_n$. Тогда правило для выбора наилучшего варианта может быть записано в виде пересечения соответствующих множеств:

$$D = C_1 \cap C_2 \cap ... \cap C_n \quad (8)$$

Операции пересечения нечеткого множества соответствует операция min, выполняемая над их функциями принадлежности:

1,
m
i=1,*n* *i*

В качестве лучшего выбирается вариант a*, имеющий наибольшее значение функции принадлежности:

$$\mu_D(a^*) = \max_{j=1,m} \mu_D(a_j) \qquad (10)$$

Рассмотрим пример выбора варианта построения СЗИ при равной важности требований.

Для определенности рассмотрим задачу выбора системы *s* защиты применительно к защите процессов и программ. Основными требованиями при выборе являются следующие требования:

к базе (полнота отражения в законодательных, нормативных и методических документах вопросов, определяющих выбор СЗИ в процессах и программах информационной системы);

к структуре (степень квалификации сотрудников, ответственных за разработку СЗИ);

к полноте и обоснованности мероприятий, обеспечивающих разработку СЗИ качественно и в заданные сроки;

к составу и характеристикам технических средств разработки СЗИ, имеющихся в распоряжении разработчика.

Пусть имеется 3 претендента – исполнителя проекта СЗИ в процессах и программах информационной системы. Претенденты оцениваются по 4 требованиям (критериям), описанным выше: C_1 — база, C_2 — структура, C_3 — меры, C_4 — средства.

В результате экспертной оценки получили следующие данные, характеризующие степень соответствия исполнителей заданным требованиям:

$C_1 = \{0,9/a_1 ; 0,7/a_2 ; 0,8/a_3\}$; $C_2 = \{0,8/a_1 ; 0,9/a_2,; 0,6/a_3,\}$; $C_3 = \{0,7/a_1 ; 0,8/a_2 ; 0,9/a_3\}$; $C_4 = \{0,8/a_1 ; 0,6/a_2 ; 0,7/a_3\}$.

В соответствии с правилом выбора получаем:

D = { min (0,9; 0,8; 0,7; 0,8/a_1); min (0,7; 0,9; 0,8; 0,6/a_2); min (0,8; 0,6; 0,9; 0,7/a_3)}= = {0,7/a1; 0,6/a2; 0,6/a_3}.

Из правила (4) следует, что наилучшим является первый исполнитель проекта a_1 = {0,9; 0,8; 0,7; 0,8}.

Выбор варианта СЗИ при различной важности требований

В случае, если требования С имеют различную важность, каждому из них приписывается число $\alpha_i \geq 0$ (чем важнее требование, тем больше α_i) и общее правило выбора принимает вид:

$$D = C_1^{\alpha_1} \cap C_2^{\alpha_2} \cap \ldots \cap C_n^{\alpha_n} \qquad (11)$$

$$\alpha_i \geq 0; i = \overline{1,n}; \sum_{i=1} \alpha_i = 1 \qquad (12)$$

Лучший вариант a* находится из соотношения:

$$\mu^D(a^*) = \max_{j=1,m} \min_{i=1,n} \mu^{C_i}(a^j) \qquad (13)$$

Рассмотрим в качестве примера выбор варианта при решении задачи защиты объектов информационной системы с точки зрения выявления потенциальных каналов утечки информации.

Пусть имеется два варианта решения задачи защиты объектов ИС (a_1, a_2).

Варианты оцениваются по тем же требованиям: C_1 — база, C_2 — структура, C_3 — меры, C_4 — средства. Важность требований определена: a_1 = 0,15; a_2 = 0,2; a_3 = 0,25; a_4 = 0,4.

Нечеткие множества, характеризирующие альтернативные варианты, имеют вид:

C_1 ={0,9/a_1 ; 0,7/a_1 }; C_2 = {0,8/a_2 ; 0,9/a_2 }; C_3 =

{0,7/a ; 0,8/a }; C =
1 2 4
{0,8/a ; 0,6/a }.
1 2

Модифицируем множества

C 0,15 = {0,9^0,15/a ; 0,7^0,15/a } = {0,984/a ; 0,984/a }
1 1 2 1 2

C 0,2 = {0,8^0,2/a ; 0,9^0,2/a } = {0,956/a ; 0,979/a } C 0,25 =
2 1 2 1 2 3

{0,7^0,25/a ; 0,8^0,25/a } = {0,915/a ; 0,946/a }
1 2 1 2

$C_4^{0,4} = \{0,8^{0,4}/a_1; 0,6^{0,4}/a_2\} = \{0,916/a_1; 0,815/a_2\}$

В соответствии с (7) получим множество

D D = {0,916/a ; 0,815/a }
1 2

Максимальное значение имеет альтернатива a — ее и выбираем в качестве
1
варианта реализации СЗИ.

Выбор варианта СЗИ по аддитивному критерию

Пусть необходимо упорядочить m вариантов СЗИ a , a , ..., a ; оцениваемых
1 2 m
по "*n*" требованиям (критериям) C , C , ..., C . Соответствующую
оценку обозначим 1 2 n
R_{ij} ; *i* =1,*m*; j =1, n относительная важность каждого
требования задается коэффициентом: $W^j \sum_{j=1}^{n} W_j =$

оценка i-го варианта вычисляется по формуле:

$$R^j = \sum_{j=1}^{n} W^j * R^{ij} \qquad (14)$$

Пусть оценки вариантов по критериям и коэффициенты относительной важности задаются функциями принадлежности соответственно: $\mu_{R^{ij}}(r_{ij})$ и $\mu_{W^j}(\omega_j)$.

Так как в данном случае R_{ij} и W_j являются нечеткими числами, R_i определяется в соответствии с формулой (14) на основе принципа обобщения. Бинарную операцию * (в данном случае это операция сложения или умножения) можно обобщить на случай нечетких чисел (например, X и Y), задаваемых функциями принадлежности $\mu_x(X)$ и $\mu_y(Y)$ соответственно. Результат обобщенной операции * - нечеткое число Z, определяемое функцией принадлежности:

$z = x^* y$

$$\mu_z(z) = \sup \min (\mu_x(x), \mu_y(y)) \qquad (15)$$

Рассмотрим случай вычисления R , когда R и W заданы функциями
i ij j
принадлежности треугольного типа (рис. 1).

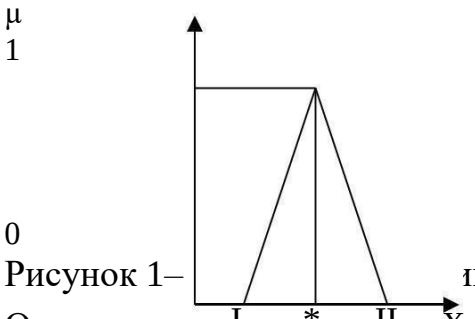


Рисунок 1– ıна нечеткого числа

Определим левую x^I и правую x^{II} границы нечеткого числа X, а также его вершину x^*:

$\forall \delta : \mu(x^I) = 0; \mu(x^I - \delta) = 0; \mu(x^I + \delta) \neq 0;$

$\forall \delta : \mu(x^{II}) = 0; \mu(x^{II} - \delta) \neq 0; \mu(x^{II} + \delta) = 0; \mu(x * 0 = 1$

Доказано, что нечеткое число Z = X*Y также определяется функцией

принадлежности треугольного вида, а границы и вершины находятся следующим образом:

$$Z^I = X^I * Y^I ; Z^{II} = X^{II} * Y^{II} ; Z^* = X^* * Y^* \qquad (16)$$

После того, как взвешенные оценки R_i получены, необходимо сравнить варианты на их основе. Для этого вводится нечеткое множество I, заданное на множестве индексов вариантов {1, 2, ..., m}. Значение соответствующей функции принадлежности интерпретируется как характеристика степени

того, насколько вариант a_i является лучшим. Значением $\mu_I(i)$ выполняется по формуле:

$$\mu_I(i) = \sup_{r_1, r_2, \ldots, r_m : r_i \geq r_{ij}} \min_{j=1,n} \mu_{R^j}(r_j) \qquad (17)$$

Рассмотрим пример сравнения двух вариантов по двум заданным требованиям (критериям), имеющим оценки, приведенные в таблице 2.

Таблица 2 – Критериальные оценки для 2-х альтернатив (вариантов)

Критерий	*Вариант*	
	1	2
1	хорошая	удовлетворительная
2	удовлетворительная	хорошая

Первый критерий определен как ОЧЕНЬ ВАЖНЫЙ, второй — ДОВОЛЬНО ВАЖНЫЙ. Термы заданы функциями принадлежности, представленными на рис. 2, 3.

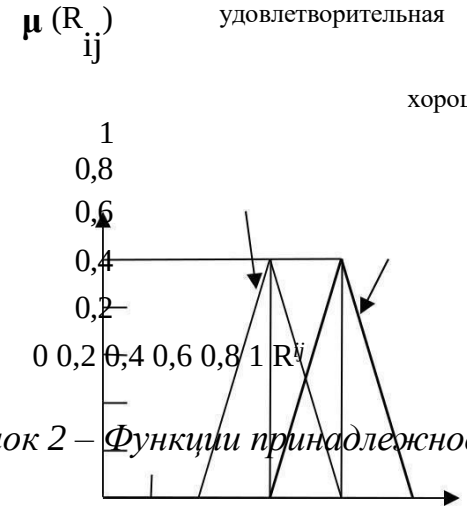


Рисунок 2 – Функции принадлежности оценок для двух вариантов

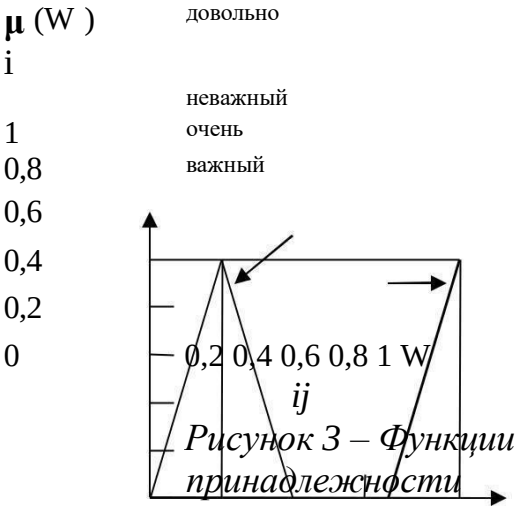


Рисунок 3 – Функции принадлежности коэффициентов важности W

$$W = \begin{matrix} 1 \\ 2 \end{matrix}$$

На основании (16) получаем:

$$R^{I} = R^{I}_{11} * W^{I}_{1} + R^{I}_{12} * W^{I}_{2} = 0,6 * 0,8 + 0,4 * 0 = 0,48$$

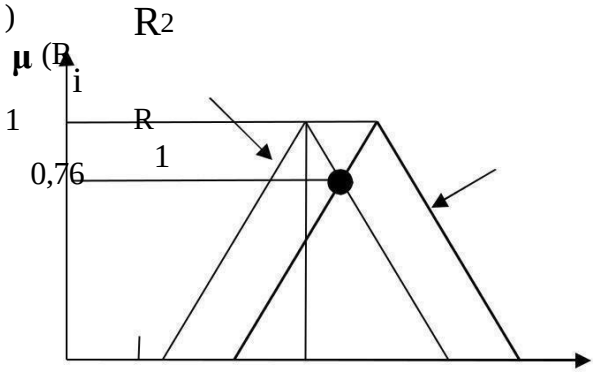
$$R^{II} = R^{II}_{11} * W^{II}_{1} + R^{II}_{12} * W^{II}_{2} = 1,0 * 1,8 + 0,8 * 0,4 = 1,32$$

$$R^{*} = R^{*}_{11} * W^{*}_{1} + R^{*}_{12} * W^{*}_{2} = 0,8 * 1,0 + 0,6 * 0,2 = 0,92$$

$$R^{I} = 0,32;\ R^{II} = 1,2;\ R^{*2} = 0,76 .$$

Аналогично

Полученные функции принадлежности изображены на рис. 4.



0 0,2 0,4 0,6 0,8 1,2 1,4 R_i

Рисунок 4 – Функции принадлежности взвешенных оценок R_1 и R_2

Тогда в соответствии с формулой (17) $\mu_I(1)=1; \mu_I(2)=0{,}76$. Следовательно наилучшим является второй вариант, а степень того, что второй вариант лучше равна 0,76.

Выбор варианта СЗИ лексикографическим методом

Применение этого метода при нечеткой информации о показателях качества (требованиях) СЗИ сводится к следующим операциям.

1°. Упорядочить требования к СЗИ по важности:

$$C_1 > C_2 > \ldots > C_j > \ldots > C_n; j=1, n$$

2°. С согласия ЛПР для каждого требования назначается величина допустимой уступки ΔC_j, j =1, n в пределах которой рассматриваемые варианты СЗИ считаются "практически равноценными".

3°. Для первого требования C_1 формируется множество "практически равноценных" вариантов, удовлетворяющих условию — множество π^1.

4°. Если $\pi 1$ — множество содержит ровно один вариант, то он и считается наилучшим. Если $\pi 1$ — множество содержит более одной альтернативы, то переходим к рассмотрению всех вариантов множества $\pi 1$, по требованию C_2.

5°. Для второго требования C^2 формируется π^2 — множество вариантов из множества π^1, удовлетворяющих условию:

$$\max_{j\in\pi^1} \mu_{C^2}(a_j) - \mu_{C^2}(a_k) \le \Delta C_2$$

$$k\in\pi^1$$

$$k\neq j$$

6°. Если π^2 — множество содержит ровно один вариант, то он и считается наилучшим; если более одного — рассматриваем эти варианты по требованию C_3 и т.д.

7°. Если все требования последовательно пересмотрены и в результате получаем π — множество $\pi = \pi^1 * \pi^2 * \ldots * \pi^n$, содержащее более одной альтернативы, то возможно применить два подхода:

– уменьшить величину допустимой уступки ΔC_j начиная с первого

по важности требования и повторить все шаги решения;

– представить ЛПР окончательный выбор лучшего варианта.

заключение рассмотрим пример выбора варианта лексикографическим методом.

Пусть в результате экспертной оценки получили следующие данные, характеризующие степень соответствия СЗИ заданным требованиям:

$C_1 = \{0{,}9/a_1 ; 0{,}9/o_1 ; 0{,}8/a_2 ; 0{,}6/a_3 ; 0{,}7/a_4 ; 0{,}8/a_5\}$

$C_2 = \{0{,}8/a_1 ; 0{,}9/a_2 ; 0{,}7/a_3 ; 0{,}8/a_4 ; 0{,}9/a_5\}$

$C_3 = \{0{,}5/a_1 ; 0{,}7/a_2 ; 0{,}8/a_3 ; 0{,}9/a_4 ; 0{,}8/a_5\}$

$C_4 = \{0{,}6/a_1 ; 0{,}7/a_2 ; 0{,}6/a_3 ; 0{,}7/a_4 ; 0{,}4/a_5\}$

1°. Требования упорядочены по важности следующим образом $C_1 > C_2 > C_3 > C_4$

2°. Зададимся величиной допустимой уступки $\Delta C_j = 0{,}1$ для всех $i = 1,4$

3°. Формируем множество π^1 по первому требованию. При максимальном значении $C_1 = 0{,}9$ и $ДС_1 = 0{,}1$ в это множество входят варианты $\pi_1 = \{a_1 , a_1 , a_3\}$.

4°. Из элементов множества π_1, формируем множество π_2 по второму требованию. При $\max_{j \in \pi_1} C_j^2 = 0{,}9$ и $C_2^2 = 0{,}1$ множество $\pi_2^2 = \{a_1 , a_2\}$.

5°. Из элементов множества $\pi^3 = \pi_1 * \pi_2$ формируем множество π^3 по третьему требованию. При $\max_{j \in \pi_1 * \pi_2} C_j^3 = 0{,}7$ и $C_2^3 = 0{,}1$ один элемент $\pi_3 = a_2$

Таким образом, наилучшим вариантом является второй вариант СЗИ.

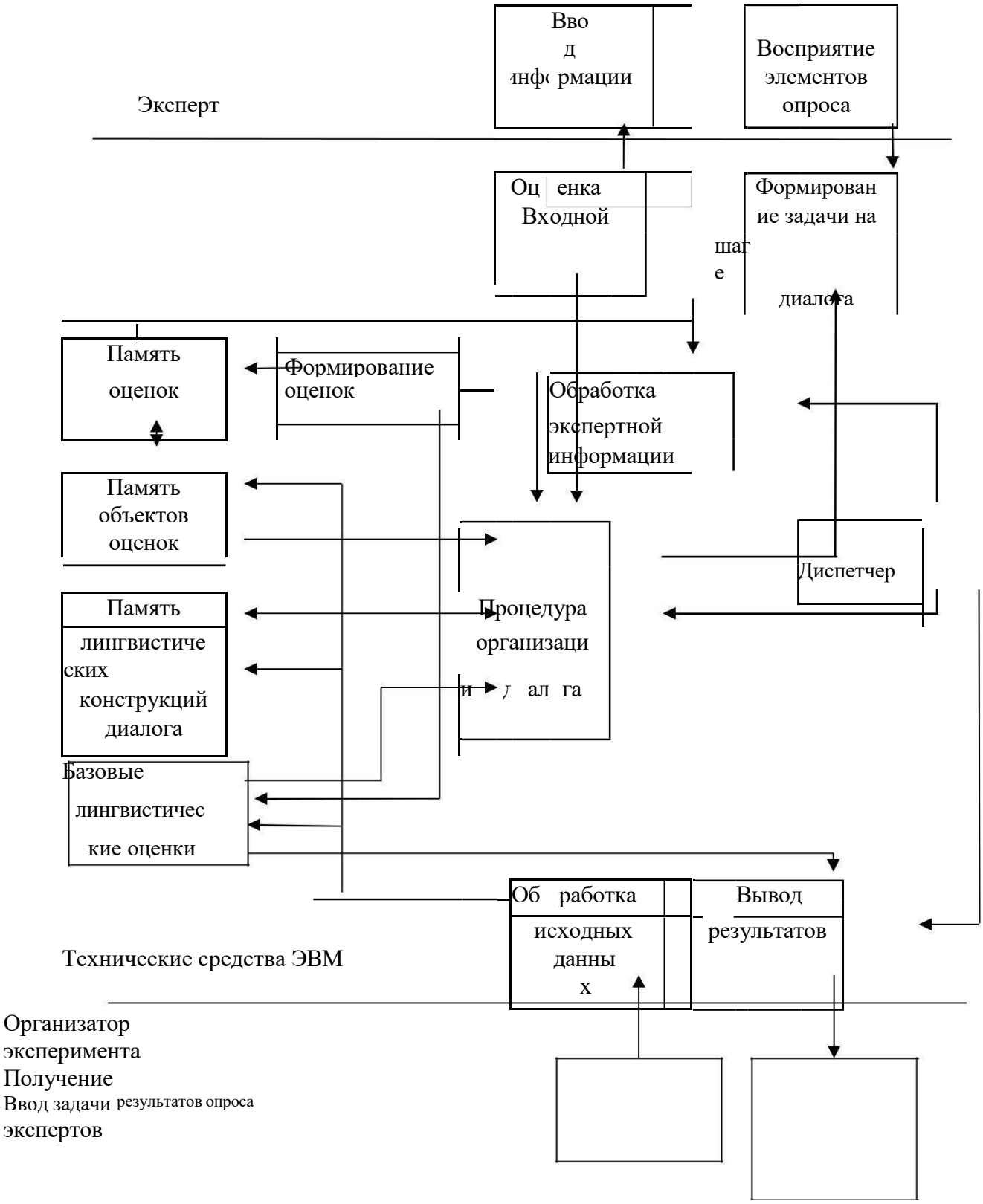


Рисунок 6 - Логическая схема получения экспертной информации с применением диалоговых средств

Практическое задание

Выделить информацию, не относящуюся к регламентированной нормативными документами. Предложить вариант системы защиты на основе использование метода экспертных оценок.

Контрольные вопросы

Что называется методом экспертных оценок?

Опишите выбор варианта СЗИ лексикографическим методом.

Дайте характеристику варианта СЗИ при равной важности требований.

Перечислите методы решения многокритериальных задач.

Нарисуйте логическую схему получения экспертной информации применением диалоговых средств.

Лабораторная работа 10.
Исследование методик расчета показателя качества системы защиты информации
Цель работы: изучить методику расчѐта показателя качества системы защиты информации.
Теоретическая часть

Модель комплексной оценки СЗИ
Модель СЗИ представлена в виде следующих основных блоков показателей:
−Блок показателей «Основы»;
−Блок показателей «Направления»;
−Блок показателей «Этапы».
Блок показателей «Основы» (O_i)
Проведенный анализ основных подходов к созданию СЗИ позволяет выделить следующую группу показателей:
$O_{1.}$ Нормативно-правовая и научная база; $O_{2.}$ Структура и задачи органов;
$O_{3.}$ Организационные меры и методы (политика безопасности); $O_{4.}$ Программно-технические способы и средства.
Значение каждого из перечисленных показателей блока «Основы» должно быть детализировано для конкретной ИС.
Блок показателей «Направления» (H_j)
Проведенный анализ существующих способов и методов защиты информации позволяет выделить следующие основные показателей создания и оценки СЗИ:
$H_{1.}$ Защита объектов корпоративных систем;
$H_{2.}$ Защита процессов, процедур и программ обработки информации; $H_{3.}$ Защита каналов связи;

$H_{4.}$ Подавление побочных электромагнитных излучений; $H_{5.}$ Управление системой защиты.

Совершенно очевидно, что каждый из показателей блока «Направлений» должен быть структурирован в зависимости от заданной глубины детализации СЗИ.

Блок показателей «Этапы» (M_k)

настоящее время рассматривают различные этапы построения СЗИ все они достаточно эффективны и позволяют решать поставленные задачи. На основе проведенного анализа предлагается рассмотрение следующих показателей создания СЗИ, подлежащих оценке:

*M*1. Определение информации, подлежащей защите;

*M*2. Выявление полного множество потенциально возможных угроз и каналов утечки информации;

*M*3. Проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;

*M*4. Определение требований к системе защиты;

*M*5. Осуществление выбора средств защиты информации и их характеристик;

*M*6. Внедрение и организация использования выбранных мер, способов и средств защиты;

*M*7. Осуществление контроля целостности и управление системой защиты.

Этапы могут быть разбиты на более детальные пункты (шаги).

Структура модели оценки СЗИ

Структура модели оценки СЗИ наглядно показана на рисунке 1. Она заключается в логическом объединении показателей блоков «ОСНОВЫ», «Направления» и «Этапы» в «Матрицу знаний (оценок)», состоящую из К элементов.

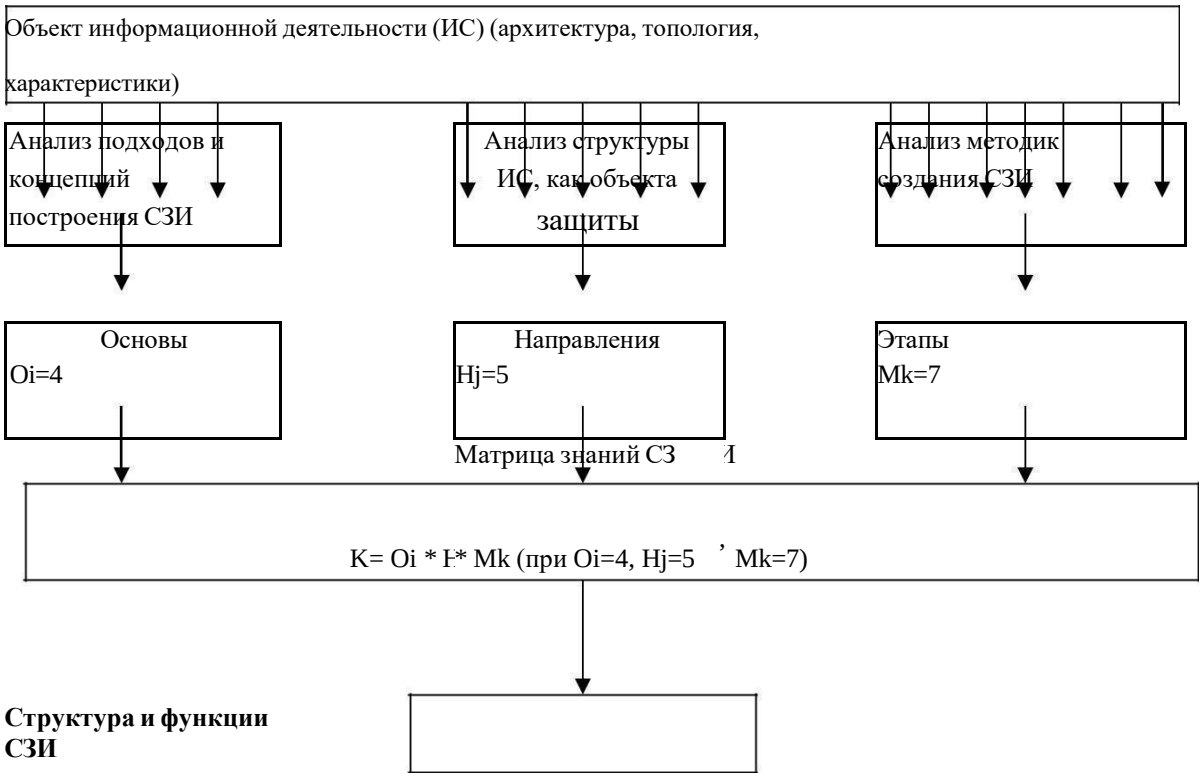


Рисунок 1 –Структура модели оценки СЗИ

Пример «Матрицы знаний (оценок)» в виде таблицы (массива) показателей наглядно представлен на рисунке 2.

	Направления >>>	010				020				030				040				050			
		Базы Операции Меры Защита объектов ИС				Защита процессов и программ				Базы Операции Меры Защита каналов связи				Базы Меры П Э М И Н				Управление системой защиты			
	Основы >>>																				
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Рисунок 2 – Пример «Матрицы знаний (оценок)»

В общем случае количество элементов «матрицы» может быть определено из соотношения

$$K = O_i \cdot H_{jk} \cdot M$$

На основе проведенного выше анализа в данном варианте (при условии, что $O_i = 4, H_j = 5, M_k = 7$) общее количество элементов «матрицы» составляет

$$K = 4 \cdot 5 \cdot 7 = 140$$

Следует обратить внимание на содержание обозначения каждого из элементов матрицы, который формируется из совокупности трех частных показателей:

Первое знакоместо обозначает номер показателя «Этапы», второе знакоместо – номер показателя «Направления», а третье знакоместо – номер показателя «Основы».

На рисунке 3 представлен пример, элемента матрицы 321, который формируется с учетом следующих показателей:

3 – Проведение оценки уязвимости и рисков (показатель № 3 блока «Этапы»);
2 – Защита процессов и программ (показатель № 2 блока «Направления»);
1 – Нормативная база (показатель № 1 блока «Основы»).
В зависимости от этапов работ по созданию СЗИ «матрица» имеет различное содержание. Другими словами это несколько одинаковых по структуре, но разных по содержанию «матриц», а именно:
1) «Матрица» полноты и качества состояний элементов СЗИ;
«Матрица» требований к СЗИ;
«Матрица» оценок эффективности функционирования элементов СЗИ.
Могут рассматриваться и другие функции этой же «матрицы», главное чтобы содержание каждого из элементов «матрицы» описывало взаимосвязь составляющих создаваемой СЗИ.

		010				020				030				04	
<<<	Направления >>>	Защита объектов ИС				Защита процессов и программ				Защита каналов связи				П Э М И	
Этапы	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Мер
100	Определение информации, подлежащей защите	011 111	012 112	013 113	014 114	021 121	022 122	023 123	024 124	031 131	032 132	033 133	034 134	041 141	042 142	0 1
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	2
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	3
400	Определение требований к СЗИ Осуществление	411	412	413	414	421	422	423	424	431	432	433	434	441	442	4
500	выбора средств защиты Внедрение и	511	512	513	514	521	522	523	524	531	532	533	534	541	542	5
600	использование выбранных мер и средств Контроль	611	612	613	614	621	622	623	624	631	632	633	634	641	642	6
700	целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	7

Рисунок 3 – Пример элемента матрицы 321

Оценки могут формироваться по различным группам элементов матрицы, в зависимости от целей проверки.
Например, отдельно можно оценить качество документации, защищенность каналов связи, качество мероприятий по выявлению угроз и каналов утечки

информации. Некоторые варианты частных оценок показаны на рисунке 4 и рисунке 5.

Основным содержанием «Матрицы полноты и качества» является вопрос «Какие из мероприятий по защите информации и в каком объеме уже выполнены?»

«Матрица требований» содержит вопрос «Какой должна быть создаваемая СЗИ?» и позволяет представить облик создаваемой СЗИ, а также сформулировать требования к ней.

«Матрица оценок» позволяет определить эффективность проводимых мероприятий по защите информации, задавая вопрос «Правильно ли строится СЗИ?» При этом используются все существующие методики оценки эффективности функционирования СЗИ.

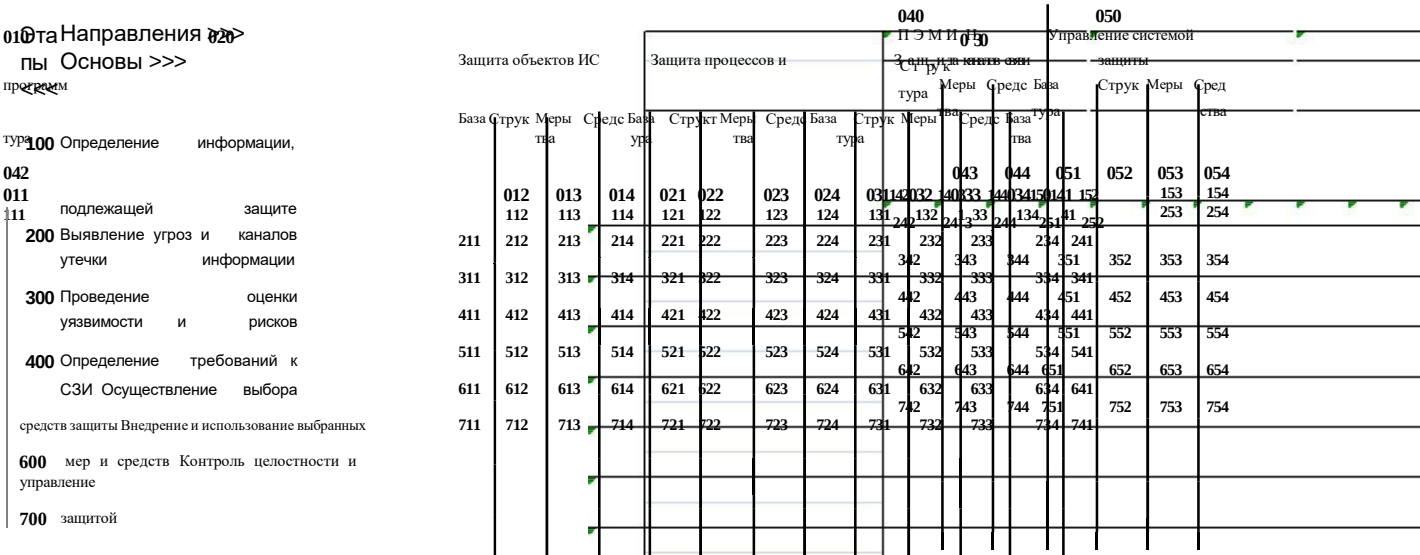


Рисунок 4 – Вариант частных оценок защищенности каналов связи

<<< Направления >>> / Этапы / Основы >>>	010 Защита объектов ИС				020 Защита процессов и программ				030 Защита каналов связи				040 ПЭМИН			
	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
100 Определение информации, подлежащей защите	011 111 211	012 112 212	013 113 213	014 114 214	021 121 221	022 122 222	023 123 223	024 124 224	031 131 231	032 132 232	033 133 233	034 134 234	041 141 241	042 142 242	043 143 243	044 144 244
200 Выявление угроз и каналов утечки информации	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344
300 Проведение оценки уязвимости и рисков	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444
400 Определение требований к СЗИ Осуществление	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544
500 выбора средств защиты Внедрение и	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644
600 использование выбранных мер и средств Контроль	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744
700 целостности и управление защитой																

<<< Направления >>> / Этапы / Основы >>>	050 Управление системой защиты			
	База	Структура	Меры	Средства
100 Определение информации, подлежащей защите	051 151 251	052 152 252	053 153 253	054 154 254
200 Выявление угроз и каналов утечки информации	351	352	353	354
300 Проведение оценки уязвимости и рисков	451	452	453	454
400 Определение требований к СЗИ Осуществление	551	552	553	554
500 выбора средств защиты Внедрение и	651	652	653	654
600 использование выбранных мер и средств Контроль	751	752	753	754
700 целостности и управление защитой				

Рисунок 5 – Вариант частных оценок качества выявления угроз

На рисунке 6 приведены вопросы «Матрицы полноты и качества» для элементов № 321, 322, 323, 324, которые объединяют показатель № 3 блока «Этапы», показатель № 2 блока «Направления» и показатели № 1, 2, 3, 4 блока «Основы»:

Элемент № 3.2.1 Насколько полно отражены в законодательных, нормативных и методических документах вопросы, определяющие порядок проведения оценки уязвимости и рисков для информации используемой в процессах и программах конкретной ИС?

Элемент № 3.2.2 Имеется ли структура органов (сотрудники), ответственная за проведение оценки уязвимости и рисков для информации используемой в процессах и программах ИС?

Элемент № 3.2.3 Определены ли режимные меры, обеспечивающие своевременное и качественное проведение оценки уязвимости и рисков для информации используемой в процессах и программах ИС?

Элемент № 3.2.4 Применяются ли технические, программные или другие средства, для обеспечения оперативности и качества проведение оценки уязвимости и рисков для информации используемой в процессах и программах ИС?

<<< Направления >>>

Этапы	Основы >>>	010 Защита объектов ИС: База	Структура	Меры	Средства	020 Защита процессов и программ: База	Структура	Меры	Средства	030 Защита каналов связи: База	Структура	Меры	Средства	База	Структура	Меры
100	Определение информации, подлежащей защите	011	012	013	014											
		111	112	113	114											
200	Выявление угроз и каналов утечки информации	211	212	213	214	021	022	023	024	031	032	033	034	041	042	0
		121	122	123	124	131	132	133	134	141	142	1				
300	Проведение оценки уязвимости и рисков	311	312	313	314	221	222	223	224	231	232	233	234	241	242	2
		411	412	413	414	321	322	323	324	331	332	333	334	341	342	3
400	Определение требований к СЗИ Осуществление	511	512	513	514	421	422	423	424	431	432	433	434	441	442	4
500	выбора средств защиты Внедрение и	611	612	613	614	521	522	523	524	531	532	533	534	541	542	5
600	использование выбранных мер и средств Контроль	711	712	713	714	621	622	623	624	631	632	633	634	641	642	6
700	целостности и управление защитой					721	722	723	724	731	732	733	734	741	742	7

Рисунок 6 – Матрица «полноты и качества» для элементов №321, 322, 323, 324.

В общем случае для «Матрицы экспертных оценок» формируется 140 вопросов (по числу ее элементов). Ответы на эти вопросы позволяют

составить полное представление о СЗИ и оценить достигнутый уровень защиты.

Показатель уровня защиты СЗИ предлагается определять методом экспертных оценок, используя положения теории нечеткой логики и нечетких утверждений.

Напомним, что структура модели оценки представлена на рисунке 1, а логическое дерево для расчета обобщенного и частных показателей уровня защиты СЗИ представлено на рисунке 7.

ес
ко
е

Ри
су
но
к7
–
И
Сз
ащ
ищ
ен
но
ст
иу
ро
вн
яо
це
нк
ив
ыв
од
ад
ер
ев
оЛ
ог
ич

нао
пре
дел
яет
сяз
ащ
ит
ыу
ров
няп
ока
зат
еля
обо
бщ
енн
ого
Вел
ичи
на

достиг
нутым
исбезо
паснос
ти.про
фильЗ
аданн
ый,без
омеха
низмы
иуслуг
и-
профи
лейзад
анных
сравне
нияпу
темпо
казате
лейчас
тныхо
снове

Уровень защиты КСЗИ (обобщенный показатель) $Q_{сзи}$ ($S_{сзи}$)

Уровень защиты объектов ИС $Q_{об}$ ($S_{об}$)

Уровень защиты процессов и программ $П_{пр}$

Уровень

каналов с

111 112. 113 114
211 212 213 214
.....
711 712 713 714

121 122 123 124
221 222 223 224
.....
721 722 723 724

131.....
.....
.....
.....
.....
731.....
.....

Матрица «защищенность объектов ИС»

Матрица «защищенность процессов и программ»

Матрица

«защище

каналов

Нормативная база

Структура органов

Комплекс мероприятий (политика безопасности)

Комплекс программных и технических средств защиты информации

111
211
…
711

112
212
…
712

112
213
…
713

114
214
…
714

Критерии безопасности

Критерии безопасности

Услуги безопасности

Механизмы безопасности

Уровень защиты от ПЭМИН $П_{пэмин}$

141..... 144
.....
.....
741..... 744

Матрица «защищенность от ПЭМИН»

Уровень гарантий защиты П г

151 152 153 154
251 252 253 254
.....
751 752 753 754

Матрица «гарантии защиты»

пасности определяются заказчиком или выбираются в соответствии с принятыми ―Критериями безопасности‖ (например Федеральные, Канадские, Общие Критерии, НД ТЗИ 2.5-004-99 или другие) в зависимости от требований, которые устанавливаются к создаваемой СЗИ.

Уровень достигнутого профиля защиты определяется экспертным путем в соответствии с теми же критериями оценки защищенности.

5. Методика оценки качества СЗИ на основе матрицы знаний

Качество СЗИ определяется степенью (полнотой) выполнения требований, предъявляемых к СЗИ. В основу оценки качества СЗИ положим исходные данные, представленные в виде матрицы знаний, заполняемой экспертами.

Заполнение матрицы знаний осуществляется на основе лингвинистических (интервальных) оценок отдельных элементов.

Особенностью частных показателей является то, что все они имеют качественный характер, т.е. не имеют точного количественного измерения. Поэтому при оценке одного и того же показателя несколькими экспертами могут возникать разные мнения. Кроме того, эксперт не всегда способен словесно оценить частный показатель, хотя интуитивно ощущает его уровень. Для преодоления этих трудностей можно оценивать частные показатели по принципу термометра (рисунок 8.а).

Удобство такого подхода состоит в том, что разные по смыслу частные показатели определяются как лингвинистические переменные, заданные на

едином универсальном множестве $U = [\underline{u}, \overline{u}]$ которым является шкала

термометра.

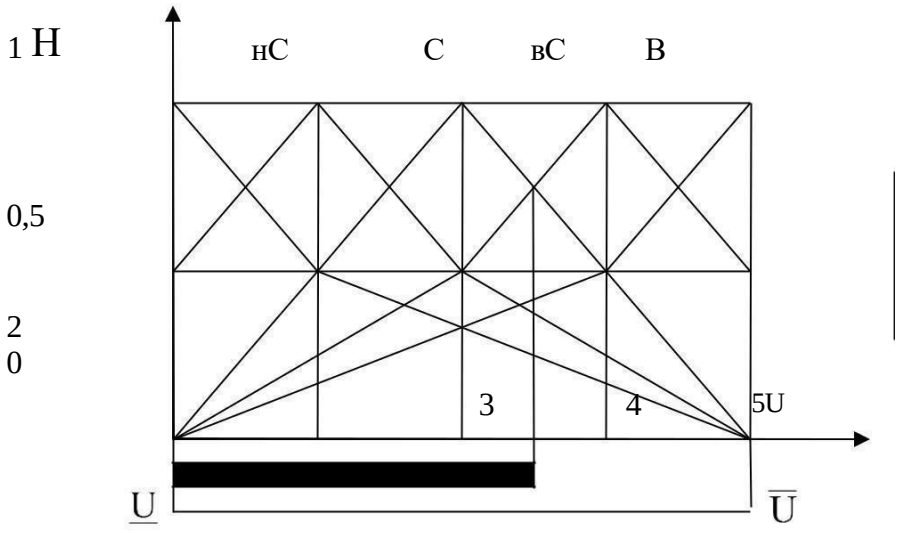


Рисунок 8.а – Оценка частных показателей по принципу термометра

Оценка частных показатели по принципу термометра дает возможность использовать в качестве показателя оценки СЗИ аддитивный показатель, который для количественной оценки качества СЗИ позволяет определить количество выполненных частных показателе. В этом случае показатель качества имеет вид:

$$Q = \frac{\sum_{k=1}^{54}\sum_{j=1}^{7}\sum_{i=1}^{kji}}{140}, \quad \begin{cases} 1, \text{ если } q_{kji} > q_{kji}^{T} \\ 0, \text{ если } q_{kji} \end{cases}$$

где $z_{kji} = \begin{cases} q_{kji} \\ > q_{kji}^{T} \end{cases}$

(А)

q_{kji} и q_{kji}^{T} – действительное и заданное значение частных показателей соответственно.

Оценка качества СЗИ имеет вид:

$$Q = \sum_{i=1m} \omega^{i} q^{i}$$

(Б)

Однако большое количество элементов матрицы знаний *(m* = 140) может привести к потере объективности определения весовых коэффициентов. Поэтому более перспективным путем является задание весовых коэффициентов столбцов, строк и направлений матрицы знаний:

$$Q = \sum_{k=1}^{5} \omega^{k} \sum_{j=1}^{4} \omega^{j} \sum_{i=1}^{7} \omega^{i} q^{kji},$$

(В)

где $\sum_{k=1}^{5} \omega^{k} = 1, \sum_{j=1}^{4} \omega^{j} = 1, \sum_{i=1}^{7} \omega^{i} = 1.$

Графическое представление степени выполнения требований приведено на рисунке 8.б.

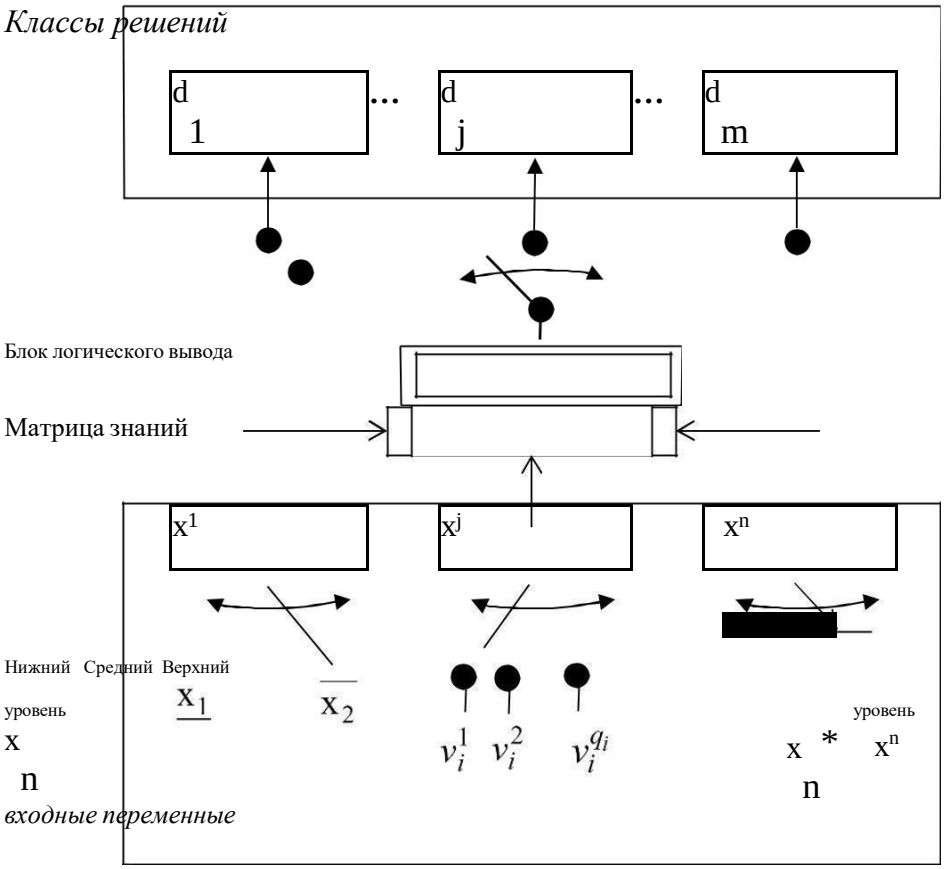


Рисунок 8.б – Схема аппроксимации для объекта с дискретным входом

Определение принадлежности СЗИ к конкретному классу проводится на основе функции принадлежности, заданной нечеткими термами классов. Результатом оценки будет вероятность принадлежности СЗИ конкретному классу.

Рассмотрим возможные варианты представления экспертных знаний и соответствующие им метол: расчета показателя качества СЗИ.

Вариант 1.а. Степень выполнения каждого требования определяется как:

¯требование выполнено Xj= 1;

требование не выполнено Xj= 0, j=1,m. Важность выполняемых требований не учитывается. Тогда качество СЗИ оценивается соотношением:

$$\sum^{m} X_j$$

$$W = \frac{j=1}{m}; 0 \le W \le 1 \qquad (1)$$

Вариант 1.6. Степень выполнения с учетом важности требований

Важность выполнения каждого требования, определяемое экспертным путем, учитывается. Тогда качество СЗИ оценивается соотношением:

$$W = \sum_{j=1}^{m} a^j x^j ; 0 \le W \le 1 \qquad (2)$$

где $0 \le a \le 1; \sum_{j=1}^{m} a^j = 1$

Вариант 2.а. Степень выполнения требований оценивается по бальной шкале.

Например, в наиболее распространенной 5-ти бальной шкале: 4 = 5 – отлично; 4 = 4 – хорошо;
4 = 3 – удовлетворительно;
4 = 2 – не удовлетворительно;
4 = 1– весьма не удовлетворительно.

С точки зрения степени удовлетворения требований бальную оценку можно интерпретировать следующим образом:
Отлично – СЗИ полностью удовлетворяет требованиям;
Хорошо – почти удовлетворяет;
Удовлетворительно – удовлетворяет в основном;
Не удовлетворительно – не удовлетворяет;
Весьма не удовлетворительно – полностью не удовлетворяет.
Качество СЗИ оценивается средним баллом.

$$B = \frac{\sum_{j=1}^{m} b^j}{m} ; 1 \le B \le 5, j = 1, m \qquad (3)$$

Вариант 2.б. Степень выполнения требований оценивается по бальной шкале, дополнительно определяется важность каждого требования

Тогда качество СЗИ определяется из выражения:

$$\overline{B} = \sum_{j=1}^{m} a^j b^j ; 1 \le \overline{B} \le 5 \qquad (4)$$

где $0 \le a \le 1; \sum_{=1}^{m} a^j = 1$

Шкала соответствия

Очень часто при бальной оценке степени выполнения требований удобно итоговую оценку иметь в шкале от 0 до 1 ($0 < Q < 1$).
Тогда надо сформировать шкалу соответствия $B \sim Q$;
$B \sim Q \quad J=1,m$
j

$$bj \sim qj;\ j = 1, \overline{m} \qquad (4.a)$$

Образец такой шкалы соответствия приведен в Таблице 1.
Таблица 1– Образец шкалы соответствия

Большая оценка	Лингвистическая оценка	Интервальная оценка
5 – отлично	(В)Полностью удовлетворяет требованиям	0,9 – 1
4 – хорошо	(ВС) Почти удовлетворяет	0,7 – 0,9
3 – удовлетворительно	(С)Удовлетворяет в основном	0,5 – 0,7
2 – не удовлетворительно	(НС) Не удовлетворяет	0,3 – 0,5
1 – весьма не удовлетворительно	(Н) Полностью не удовлетворяет	0 – 0,3

Оценка качества СЗИ производится по формулам аналогичным (3) и (4).

$$Q = \frac{\sum_{j=1}^{m} j}{m} \qquad (5)$$

$$Q_j = \frac{\sum_{j=1}^{m} a^j q}{m} \qquad (6)$$

7. Лингвистическая приемная

Пусть лингвистическая переменная «Качество СЗИ» определена на универсальном, множестве вариантов СЗИ

$u^i ; i = 1, n$

(*1)

Уровень качества СЗИ будем оценивать термами (В, ВС, С, НС, Н), приведенными в табл. 1.

Пусть далее экспертным путем одним из методов, описанных в главе 6, получены функции принадлежности

$\mu(u_{ij})$

(*2)

Тогда, используя функции принадлежности с помощью табл. 1. Можно получить оценку качества СЗИ либо в виде оценки:

$$B_i = \frac{\sum_{j=1}^{m} B_{ij}}{m} = \frac{\sum_{j=1}^{m} b_j}{m} \qquad (7)$$

$$B_i = \sum_{j=1}^{m} \alpha_j \sum_{b_j=1}^{5} b_j \mu(u_{ij} b_j) \qquad (8)$$

8. Оценка качества СЗИ на основе анализа профиля безопасности

Под профилем безопасности в дальнейшем будем понимать графическое представление степени выполнения требований в системе координат:

по горизонтали – перечень требований, предъявляемых к СЗИ;

по вертикали – степень выполнения каждого требования.
Степень выполнения каждого требования рассчитывается в соответствии с формулами (1)...(10).
Рассмотрим частный (наиболее удобный с нашей точки зрения) случай, когда степень выполнения требований задается в шкале $0 < Q < 1$; $J = 1,m$.
При этом целесообразно рассматривать два профиля безопасности: требуемый и реально достигнутый.
Для построения требуемого профиля безопасности используются предварительно заданные экспертами значения:

$$0 \le Q_j^{TP} \le 1, j=1,m \qquad (*3)$$

Исходные данные для построения требуемого профиля безопасности представлены в виде уже знакомой матрицы знаний.

9. Пример оценки качества

Как указывалось ранее, качество СЗИ определяется степенью (полнотой) выполнения требований к СЗИ. Исходные данные, представлены в виде частных матриц знаний, заполненных экспертами по соответствующим направлениям защиты (рис. 9– 13).
На рис. 9 представлены данные для оценки ***защищенности объектов ИС*** (первое направление защиты). Поясним используемые обозначения:
Номер этапа с 1 по 7 (см. блок показателей «Этапы»).
Перечень показателей *(m)* для соответствующих элементов матрицы (от 1 до 28).
Коэффициенты важности (a_j), которые определяются для показателей каждого из этапов.
Показатели требуемого профиля безопасности *(Qmp)*. Для всех показателей установлено значение 0,65. Графически требуемый профиль изображен на диаграмме «Сравнение профилей защиты» (рисунок 9) в виде прямой линии на уровне 0,65.

•Показатели достигнутого профиля безопасности *($Q_д$)*. Их значения определены экспертами и графически изображены на диаграмме «Сравнение профилей защиты» в виде ломанной линии.

6. Показатели достигнутого профиля безопасности с учетом коэффициентов важности ($Q_{\partial aj}$).

Сравнение профилей (S_{np}), которое производится следующим образом:

(S^{np}) = 1 – если значение показателя достигнутого профиля безопасности равно или превышает значение показателя заданного;

(S_{np}) = 0 – если значение показателя достигнутого профиля безопасности ниже значение показателя заданного.

Графически этот процесс представлен на диаграмме «Оценка достигнутого профиля безопасности» (рисунок 9).

Степень выполнения групп требований ($Q_{груп}$) в данном примере определяется с учетом коэффициентов важности ($Q_{дaj}$) для каждого из этапов: 1-0,68, 2-0,65, 3-0,60, 4-0,80, 5-0,80, 6-0,65, 7-0,80. Графически эти значения изображены на диаграмме «Оценка этапов» (рис. 9).

Качественная оценка *(Q)* определяется исходя из значений показателей ($Q_{груп}$) вычисленных для соответствующих этапов. В нашем случае:

$Q_{груп}$ =0,71

Количественная оценка *(S)* определятся путем подсчета значений *($S_{пр}$),* а именно нулей и единиц полученных при сравнении профилей. Это более грубая оценка, определяющая количество выполненных (достигнутых) требований:

S = 0,68

Другими словами в рассматриваемой ИС выполнено 68% требований по защите информации. Правда не известно насколько эти требования важны.

Аналогичным образом производится оценка для других направлений защиты. Результаты представлены на рисунках 10-13.

Далее, объединив частные показатели (по направлениям) в обобщенный показатель, получаем результирующий профиль безопасности и его графическое изображение (рисунок 14). Обратите внимание на то, что требования 11, 12, 21 и 22 не выполнены вообще ни в одном из направлений защиты. Требования 1, 3,4,5,9,10 и др. выполнены не по всем направлениям. Определить какие группы требований по каким направлениям выполнены можно с помощью диаграммы (рисунок 15).

этапа №	Перечень показателей	№элементам атрицы	Коэффициент важности	Важностьпоказателя	Безважностидостигнуты	Qд x aj	Сравнениепрофилей	Qгруп	Качественная оценка	Количественная оценка
	m	№	a_j	Q mp	Qд	Q *daj*	S пр	Q *груп*	Q	S
1	1.	111	0,5	0,65	0,7	0,35	1	0,68		
	2.	112	0,2	0,65	0,8	0,16	1			
	3.	113	0,15	0,65	0,5	0,075	0			
	4.	114	0,15	0,65	0,6	0,09	0			
2	5.	211	0,5	0,65	0,5	0,25	0	0,65		
	6.	212	0,2	0,65	0,8	0,16	1			
	7.	213	0,15	0,65	0,8	0,12	1			
	8.	214	0,15	0,65	0,8	0,12	1		**0,71**	**0,68**
3	9.	311	0,25	0,65	0,6	0,15	0	0,60		
	10.	312	0,25	0,65	0,6	0,15	0			
	11.	313	0,25	0,65	0,6	0,15	0			
	12.	314	0,25	0,65	0,6	0,15	0			
4	13.	411	0,5	0,65	0,8	0,4	1	0,80		
	14.	412	0,2	0,65	0,8	0,16	1			

	15.	413	0,15	0,65	0,8	0,12	1			

	16.	414	0,15	0,65	0,8	0,12	1			
5	17.	511	0,25	0,65	0,8	0,2	1	0,80		
	18.	512	0,25	0,65	0,8	0,2	1			
	19.	513	0,25	0,65	0,8	0,2	1			
	20.	514	0,25	0,65	0,8	0,2	1			
6	21.	611	0,25	0,65	0,5	0,125	0	0,65		
	22.	612	0,25	0,65	0,5	0,125	0			
	23.	613	0,25	0,65	0,8	0,2	1			
	24.	614	0,25	0,65	0,8	0,2	1			
7	25.	711	0,5	0,65	0,8	0,4	1	0,80		
	26.	712	0,2	0,65	0,8	0,16	1			
	27.	713	0,15	0,65	0,8	0,12	1			
	28.	714	0,15	0,65	0,8	0,12	1			

Рисунок 9 – Оценка защищенности объектов ИС

№ этапа	Переченьпоказателей	№элементаматрицы	Коэффициентважности		Безопасностидостигнуты	Qд x aj	Сравнениепрофилей		Качественная оценка	Количественная оценка
	m	№	a *j*	Q mp	Q*д*	Q *даj*	S пр	Q *груп*	Q	S
1	1.	121	0,5	0,7	0,9	0,45	1	0,90		
	2.	122	0,2	0,7	0,9	0,18	1			
	3.	123	0,15	0,7	0,9	0,135	1			
	4.	124	0,15	0,7	0,9	0,135	1			
2	5.	221	0,25	0,7	0,9	0,225	1	0,90		
	6.	222	0,25	0,7	0,9	0,225	1			
	7.	223	0,25	0,7	0,9	0,225	1			
	8.	224	0,25	0,7	0,9	0,225	1			
3	9.	321	0,25	0,7	0,9	0,225	1	0,68		
	10.	322	0,25	0,7	0,6	0,15	0			
	11.	323	0,25	0,7	0,6	0,15	0			
	12.	324	0,25	0,7	0,6	0,15	0			
4	13.	421	0,25	0,7	0,8	0,2	1	0,80	**0,79**	**0,82**
	14.	422	0,25	0,7	0,8	0,2	1			
	15.	423	0,25	0,7	0,8	0,2	1			
	16.	424	0,25	0,7	0,8	0,2	1			
5	17.	521	0,25	0,7	0,8	0,2	1	0,80		
	18.	522	0,25	0,7	0,8	0,2	1			
	19.	523	0,25	0,7	0,8	0,2	1			
	20.	524	0,25	0,7	0,8	0,2	1			
6	21.	621	0,25	0,7	0,5	0,125	0	0,65		
	22.	622	0,25	0,7	0,5	0,125	0			
	23.	623	0,25	0,7	0,8	0,2	1			
	24.	624	0,25	0,7	0,8	0,2	1			
7	25.	721	0,25	0,7	0,8	0,2	1	0,80		
	26.	722	0,25	0,7	0,8	0,2	1			
	27.	723	0,25	0,7	0,8	0,2	1			

	28.	724	0,25	0,7	0,8	0,2	1			

Рисунок 10 – Оценка защищенности процессов и программ ИС

№ этапа	Перечень показателей	№ элемента матрицы	Коэффициент важности			Qд x aj	Сравнение профилей		Качественная оценка	Количественная оценка
	m	№	a_j	Q mp	Q*д*	Q *даj*	S пр	Q *груп*	Q	S
1	1.	131	0,5	0,8	0,7	0,35	0	0,68		
	2.	132	0,2	0,8	0,8	0,16	1			
	3.	133	0,15	0,8	0,5	0,075	0			
	4.	134	0,15	0,8	0,6	0,09	0			
2	5.	231	0,25	0,8	0,5	0,125	0	0,73		
	6.	232	0,25	0,8	0,8	0,2	1			
	7.	233	0,25	0,8	0,8	0,2	1			
	8.	234	0,25	0,8	0,8	0,2	1			
3	9.	331	0,25	0,8	0,6	0,15	0	0,60		
	10.	332	0,25	0,8	0,6	0,15	0			
	11.	333	0,25	0,8	0,6	0,15	0			
	12.	334	0,25	0,8	0,6	0,15	0			
4	13.	431	0,25	0,8	0,8	0,2	1	0,70	**0,67**	**0,39**
	14.	432	0,25	0,8	0,8	0,2	1			
	15.	433	0,25	0,8	0,6	0,15	0			
	16.	434	0,25	0,8	0,6	0,15	0			
5	17.	531	0,25	0,8	0,6	0,15	0	0,65		
	18.	532	0,25	0,8	0,6	0,15	0			
	19.	533	0,25	0,8	0,6	0,15	0			
	20.	534	0,25	0,8	0,8	0,2	1			
6	21.	631	0,25	0,8	0,5	0,125	0	0,65		
	22.	632	0,25	0,8	0,5	0,125	0			
	23.	633	0,25	0,8	0,8	0,2	1			
	24.	634	0,25	0,8	0,8	0,2	1			
7	25.	731	0,25	0,8	0,8	0,2	1	0,68		
	26.	732	0,25	0,8	0,6	0,15	0			
	27.	733	0,25	0,8	0,5	0,125	0			
	28.	734	0,25	0,8	0,8	0,2	1			

Рисунок 11 – Оценка защищенности каналов связи ИС

№ этапа	Перечень показателей	№ элемента матрицы	Коэффициент важности			Qд x aj	Сравнение профилей		Качественная оценка	Количественная оценка
	m	№	a_j	Q mp	Q*д*	Q *даj*	S пр	Q *груп*	Q	S
1	1.	141	0,5	0,75	0,7	0,35	0	0,68		
	2.	142	0,2	0,75	0,8	0,16	1			
	3.	143	0,15	0,75	0,5	0,075	0			
	4.	144	0,15	0,75	0,6	0,09	0			
2	5.	241	0,25	0,75	0,5	0,125	0	0,73	**0,72**	**0,64**
	6.	242	0,25	0,75	0,8	0,2	1			
	7.	243	0,25	0,75	0,8	0,2	1			
	8.	244	0,25	0,75	0,8	0,2	1			

3	9.	341	0,25	0,75	0,6	0,15	0	0,60		
	10.	342	0,25	0,75	0,6	0,15	0			

	11.	343	0,25	0,75	0,6	0,15	0			
	12.	344	0,25	0,75	0,6	0,15	0			
4	13.	441	0,25	0,75	0,8	0,2	1	0,80		
	14.	442	0,25	0,75	0,8	0,2	1			
	15.	443	0,25	0,75	0,8	0,2	1			
	16.	444	0,25	0,75	0,8	0,2	1			
5	17.	541	0,25	0,75	0,8	0,2	1	0,80		
	18.	542	0,25	0,75	0,8	0,2	1			
	19.	543	0,25	0,75	0,8	0,2	1			
	20.	544	0,25	0,75	0,8	0,2	1			
6	21.	641	0,25	0,75	0,5	0,125	0	0,65		
	22.	642	0,25	0,75	0,5	0,125	0			
	23.	643	0,25	0,75	0,8	0,2	1			
	24.	644	0,25	0,75	0,8	0,2	1			
7	25.	741	0,25	0,75	0,8	0,2	1	0,80		
	26.	742	0,25	0,75	0,8	0,2	1			
	27.	743	0,25	0,75	0,8	0,2	1			
	28.	744	0,25	0,75	0,8	0,2	1			

Рисунок 12 – Оценка защищенности от утечки по техническим каналам (ПЭМИН)

№ этапа	Переченьпоказателей	№элементаматрицы	Коэффициентважности	[illegible]	Безопасностидостигнуты	Qд x aj	Сравнениепрофилей	Степеньвыполнения группттребований	Качественная оценка	Количественная оценка
	m	№	aj	Q mp	Q*д*	Q *daj*	S пр	Q *груп*	Q	S
1	1.	151	0,5	0,6	0,7	0,35	1	0,68		
	2.	152	0,2	0,6	0,8	0,16	1			
	3.	153	0,15	0,6	0,5	0,075	0			
	4.	154	0,15	0,6	0,6	0,09	1			
2	5.	251	0,25	0,6	0,5	0,125	0	0,73		
	6.	252	0,25	0,6	0,8	0,2	1			
	7.	253	0,25	0,6	0,8	0,2	1			
	8.	254	0,25	0,6	0,8	0,2	1			
3	9.	351	0,5	0,6	0,6	0,3	1	0,59		
	10.	352	0,2	0,6	0,6	0,12	1			
	11.	353	0,15	0,6	0,5	0,075	0		**0,72**	**0,79**
	12.	354	0,15	0,6	0,6	0,09	0			
4	13.	451	0,25	0,6	0,8	0,2	1	0,80		
	14.	452	0,25	0,6	0,8	0,2	1			
	15.	453	0,25	0,6	0,8	0,2	1			
	16.	454	0,25	0,6	0,8	0,2	1			
5	17.	551	0,5	0,6	0,8	0,4	1	0,80		
	18.	552	0,2	0,6	0,8	0,16	1			
	19.	553	0,15	0,6	0,8	0,12	1			
	20.	554	0,15	0,6	0,8	0,12	1			
6	21.	651	0,25	0,6	0,5	0,125	0	0,65		
	22.	652	0,25	0,6	0,5	0,125	0			
	23.	653	0,25	0,6	0,8	0,2	1			

	24.	654	0,25	0,6	0,8	0,2	1			
7	25.	751	0,5	0,6	0,8	0,4	1	0,80		

	26.	752	0,2	0,6	0,8	0,16	1			
	27.	753	0,15	0,6	0,8	0,12	1			
	28.	754	0,15	0,6	0,8	0,12	1			

Рисунок 13 – Оценка защищенности элементов системы защиты (управление и контроль)

Табличное представление обобщенных количественных оценок

	Направления защиты					Q *сзи*
	1	2	3	4	5	
1	1,00	1,00	0,00	0,00	1,00	0,60
2	1,00	1,00	1,00	1,00	1,00	1,00
3	0,00	1,00	0,00	0,00	0,00	0,20
4	0,00	1,00	0,00	0,00	1,00	0,40
5	0,00	1,00	0,00	0,00	0,00	0,20
6	1,00	1,00	1,00	1,00	1,00	1,00
7	1,00	1,00	1,00	1,00	1,00	1,00
8	1,00	1,00	1,00	1,00	1,00	1,00
9	0,00	1,00	0,00	0,00	1,00	0,40
10	0,00	0,00	0,00	0,00	1,00	0,20
11	0,00	0,00	0,00	0,00	0,00	0,00
12	0,00	0,00	0,00	0,00	0,00	0,00
13	1,00	1,00	1,00	1,00	1,00	1,00
14	1,00	1,00	1,00	1,00	1,00	1,00
15	1,00	1,00	0,00	1,00	1,00	0,80
16	1,00	1,00	0,00	1,00	1,00	0,80
17	1,00	1,00	0,00	1,00	1,00	0,80
18	1,00	1,00	0,00	1,00	1,00	0,80
19	1,00	1,00	0,00	1,00	1,00	0,80
20	1,00	1,00	1,00	1,00	1,00	1,00
21	0,00	0,00	0,00	0,00	0,00	0,00
22	0,00	0,00	0,00	0,00	0,00	0,00
23	1,00	1,00	1,00	1,00	1,00	1,00
24	1,00	1,00	1,00	1,00	1,00	1,00
25	1,00	1,00	1,00	1,00	1,00	1,00
26	1,00	1,00	0,00	1,00	1,00	0,80
27	1,00	1,00	0,00	1,00	1,00	0,80
28	1,00	1,00	1,00	1,00	1,00	1,00

Рисунок 14 – Достигнутый суммарный профиль безопасности (количественная оценка)

Обобщенные показатели уровня защищенности (качественный и количественный) представлены на рисунке 16. Превышение величины качественного показателя над количественным, свидетельствует о том, что выполненные требования более важны по своему значению чем невыполненные.

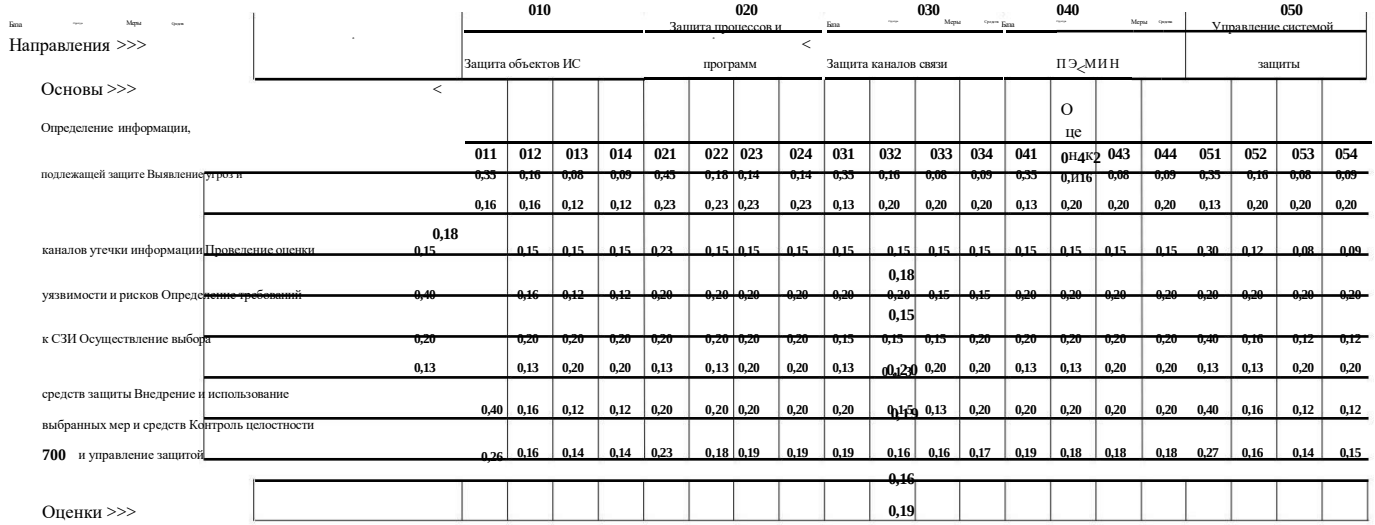
На рисунках 17 и 18 представлены матрицы количественных и качественных оценок уровня защищенности, позволяющие наглядно оценить степень выполнения требований по защите информации. Это дает возможность определить сильные и слабые места в СЗИ.

	Направления защиты					
	1	2	3	4	5	
1	1,00	1,00	0,00	0,00	1,00	
2	1,00	1,00	1,00	1,00	1,00	
3	0,00	1,00	0,00	0,00	0,00	
4	0,00	1,00	0,00	0,00	1,00	
5	0,00	1,00	0,00	0,00	0,00	
6	1,00	1,00	1,00	1,00	1,00	
7	1,00	1,00	1,00	1,00	1,00	
8	1,00	1,00	1,00	1,00	1,00	
9	0,00	1,00	0,00	0,00	1,00	
10	0,00	0,00	0,00	0,00	1,00	
11	0,00	0,00	0,00	0,00	0,00	0,00
12	0,00	0,00	0,00	0,00	0,00	0,00
13	1,00	1,00	1,00	1,00	1,00	1,00
14	1,00	1,00	1,00	1,00	1,00	1,00
15	1,00	1,00	0,00	1,00	1,00	0,80
16	1,00	1,00	0,00	1,00	1,00	0,80
17	1,00	1,00	0,00	1,00	1,00	0,80
18	1,00	1,00	0,00	1,00	1,00	0,80
19	1,00	1,00	0,00	1,00	1,00	0,80
20	1,00	1,00	1,00	1,00	1,00	1,00
21	0,00	0,00	0,00	0,00	0,00	0,00
22	0,00	0,00	0,00	0,00	0,00	0,00
23	1,00	1,00	1,00	1,00	1,00	
24	1,00	1,00	1,00	1,00	1,00	1,00
25	1,00	1,00	1,00	1,00	1,00	
26	1,00	1,00	0,00	1,00	1,00	
27	1,00	1,00	0,00	1,00	1,00	
28	1,00	1,00	1,00	1,00	1,00	

Рисунок 15 – Количественные показатели выполнения требований по защите информации

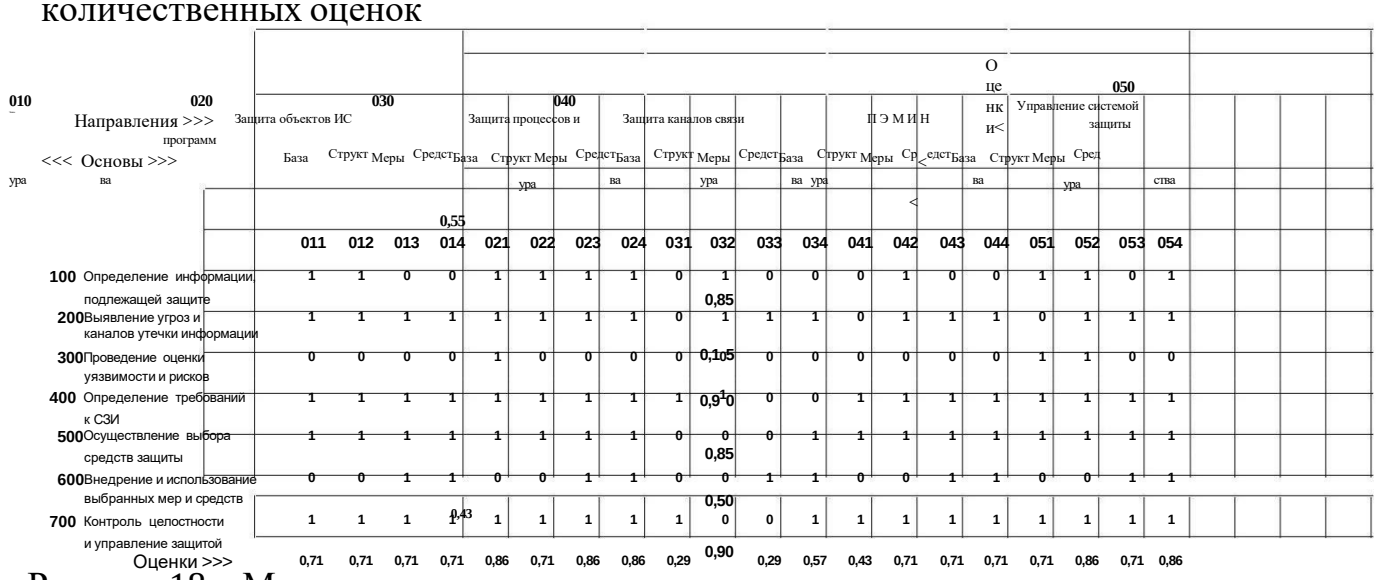
Показатели	Направления защиты					Q.сзи
	1	2	3	4	5	
	Коэффициенты важности по направлениям					
	0,3	0,1	0,2	0,1	0,3	
Количественный	0,68	0,82	0,39	0,64	0,79	0,66
Качественный	0,71	0,79	0,67	0,72	0,72	0,71

Рисунок 16 – Обобщенные показатели уровня защищенности ИС



Направления >>>	010 Защита объектов ИС				020 Защита процессов и программ				030 Защита каналов связи				040 ПЭМИН				050 Управление системой защиты			
Основы >>>	011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
Определение информации, подлежащей защите	0,55	0,16	0,08	0,09	0,45	0,18	0,14	0,14	0,55	0,16	0,08	0,09	0,55	0,16	0,08	0,09	0,55	0,16	0,08	0,09
Выявление угроз и каналов утечки информации	0,16	0,16	0,12	0,12	0,23	0,23	0,23	0,23	0,13	0,20	0,20	0,20	0,13	0,20	0,20	0,20	0,13	0,20	0,20	0,20
Проведение оценки уязвимости и рисков	0,18	0,15	0,15	0,15	0,23	0,15	0,15	0,15	0,15	0,15	0,15	0,15	0,15	0,15	0,15	0,15	0,30	0,12	0,08	0,09
Определение требований к СЗИ	0,40	0,16	0,12	0,12	0,20	0,20	0,20	0,20	0,20	0,20	0,15	0,15	0,20	0,20	0,20	0,20	0,20	0,20	0,20	0,20
Осуществление выбора средств защиты	0,20	0,20	0,20	0,20	0,20	0,20	0,20	0,20	0,15	0,15	0,15	0,20	0,20	0,20	0,20	0,20	0,40	0,16	0,12	0,12
Внедрение и использование выбранных мер и средств	0,13	0,13	0,20	0,20	0,13	0,13	0,20	0,20	0,13	0,20	0,20	0,20	0,13	0,13	0,20	0,20	0,13	0,13	0,20	0,20
Контроль целостности и управление защитой	0,40	0,16	0,12	0,12	0,20	0,20	0,20	0,20	0,20	0,15	0,13	0,20	0,20	0,20	0,20	0,20	0,40	0,16	0,12	0,12
700	0,26	0,16	0,14	0,14	0,23	0,18	0,19	0,19	0,19	0,16	0,16	0,17	0,19	0,18	0,18	0,18	0,27	0,16	0,14	0,15
Оценки >>>																				

Рисунок 17 – Матрица количественных оценок



Направления >>>	010 Защита объектов ИС				020 Защита процессов и программ				030 Защита каналов связи				040 ПЭМИН				050 Управление системой защиты			
<<< Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
	011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100 Определение информации, подлежащей защите	1	1	0	0	1	1	1	1	0	1	0	0	0	1	0	0	1	1	0	1
200 Выявление угроз и каналов утечки информации	1	1	1	1	1	1	1	1	0	1	1	1	0	1	1	1	0	1	1	1
300 Проведение оценки уязвимости и рисков	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0
400 Определение требований к СЗИ	1	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	1
500 Осуществление выбора средств защиты	1	1	1	1	1	1	1	1	0	0	0	1	1	1	1	1	1	1	1	1
600 Внедрение и использование выбранных мер и средств	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
700 Контроль целостности и управление защитой	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	1	1
Оценки >>>	0,71	0,71	0,71	0,71	0,86	0,71	0,86	0,86	0,29	0,90	0,29	0,57	0,43	0,71	0,71	0,71	0,71	0,86	0,71	0,86

Рисунок 18 – Матрица качественных оценок

Практическое задание

Проведите оценку исходной защищѐнности объекта информатизации.

Контрольные вопросы

Нарисуйте структуру модели оценки СЗИ.

Опишите принцип формирования матрицы знаний (оценок).

Опишите принцип формирования частных оценок защищенности каналов связи

Что называется «Матрица полноты и качества»?

Нарисуйтелогическоедеревовыводаоценкиуровня защищенности ИС.

Лабораторная работа 11.

Изучение методов построения комплексной системы организационных и технических мер по защите информации

Цель работы: изучить методы построения КСЗИ организационных и технических мер по защите информации.

Теоретическая часть

Под информационной безопасностью понимается защищенность информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре.

Существует множество причин и мотивов, по которым одни люди хотят шпионить за другими. Имея немного денег и старание, злоумышленники могут организовать ряд каналов утечки сведений, используя собственную изобретательность и (или) халатность владельца информации. Задачи информационной безопасности сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий.

Для построения системы надежной **защиты информации** необходимо выявить все возможные угрозы безопасности, оценить их последствия, определить необходимые меры и средства защиты, оценить их эффективность. Оценка рисков производится квалифицированными специалистами с помощью различных инструментальных средств, а также методов моделирования процессов защиты информации. На основании результатов анализа выявляются наиболее высокие риски, переводящих потенциальную угрозу в разряд реально опасных и, следовательно, требующих принятия дополнительных мер обеспечения безопасности.

Информация может иметь несколько уровней значимости, важности, ценности, что предусматривает соответственно наличие нескольких уровней ее конфиденциальности. Наличие разных уровней доступа к информации

предполагает различную степень обеспечения каждого из свойств безопасности информации – *конфиденциальность,*

целостность и *доступность*.

Анализ системы защиты информации, моделирование вероятных угроз позволяет определить необходимые меры защиты. При построении системы защиты информации необходимо строго соблюдать пропорцию между стоимостью системы защиты и степенью ценности информации. И только располагая сведениями о рынке открытых отечественных и зарубежных технических средств несанкционированного съема информации, возможно определить необходимые меры и способы защиты информации. Это одна из самых сложных задач в проектировании системы защиты коммерческих секретов.

При возникновении различных угроз от них приходится защищаться. Для того чтобы оценить вероятные угрозы, следует перечислить и основные категории источников конфиденциальной информации – это могут быть люди, документы, публикации, технические носители, технические средства обеспечения производственной и трудовой деятельности, продукция, промышленные и производственные отходы и т. д. Кроме того, к возможным каналам утечки информации следует отнести совместную деятельность с другими фирмами; участие в переговорах; фиктивные запросы со стороны о возможности работать в фирме на различных должностях; посещения гостей фирмы; знания торговых представителей фирмы о характеристиках изделия; излишнюю рекламу; поставки смежников; консультации специалистов со стороны; публикации в печати и выступления, конференции, симпозиумы и т. д.; разговоры в нерабочих помещениях; правоохранительные органы; «обиженных» сотрудников предприятия и т. п.

Все возможные **способы защиты информации** сводятся к нескольким основным методикам:

-воспрепятствование непосредственному проникновению к источнику информации с помощью инженерных конструкций технических средств охраны;
⁻скрытие достоверной информации;
-предоставление ложной информации.

Упрощенно принято выделять две формы восприятия информации – акустическую и зрительную (сигнальную). Акустическая информация в потоках сообщений носит преобладающий характер. Понятие зрительной информации весьма обширно, поэтому ее следует подразделять на *объемно-*

видовую и *аналогово-цифровую*.

Самыми распространенными способами несанкционированного получения конфиденциальной информации являются:
⁻прослушивание помещений с помощью технических средств;
⁻наблюдение (в т. ч. фотографирование и видеосъемка);
перехват информации с использованием средств радиомониторинга информативных побочных излучений технических средств;
⁻хищение носителей информации и производственных отходов;
чтение остаточной информации в запоминающих устройствах системы после выполнения санкционированного запроса, копирование носителей информации;
несанкционированное использование терминалов зарегистрированных пользователей с помощью хищения паролей;
внесение изменений, дезинформация, физические и программные методы разрушения (уничтожения) информации.

Современная концепция защиты информации, циркулирующей в помещениях или технических системах коммерческого объекта, требует не периодического, а постоянного контроля в зоне расположения объекта. Защита информации включает в себя целый комплекс организационных и

технических мер по обеспечению информационной безопасности техническими средствами. Она должна решать такие задачи, как: предотвращение доступа злоумышленника к источникам информации с целью ее уничтожения, хищения или изменения;
защита носителей информации от уничтожения в результате различных воздействий;
− предотвращение утечки информации по различным техническим каналам . Способы и средства решения первых двух задач не отличаются от способов и средств защиты любых материальных ценностей, третья задача
решается исключительно способами и средствами инженерно-технической защиты информации.

Разработка и внедрение комплексных систем защиты информации

Разработка и внедрение системы защиты информации осуществляется соответствии с требованиями **Федерального закона РФ от 27 июля 2006 г. № 149-ФЗ** "Об информации, информационных технологиях и защите информации" и нормативными документами РФ в области защиты информации, с последующей аттестацией в системе сертификации ФСТЭК России.
Цели и задачи, решаемые в ходе оказания услуг Основной целью
выполнения работ является обеспечение соответствия

объекта информатизации (ОИ) организации требованиям Федерального закона РФ № 149-ФЗ "Об информации, информационных технологиях и защите информации".
ходе выполнения работ решаются следующие задачи:
разрабатываются методическое руководство и конкретные требования по защите информации;
разрабатывается аналитическое обоснование необходимости создания системы защиты информации (СЗИ);

согласовывается выбор основных и вспомогательных технических средств и систем (ОТСС и ВТСС), технических и программных средств защиты информации (ЗИ);
организуются работы по выявлению возможных каналов утечки информации и нарушения целостности защищаемой информации, производится аттестация объекта информатизации.

Этапы создания системы защиты информации:

1. Предпроектный этап, включающий предпроектное обследование объекта информатизации, разработку аналитического обоснования необходимости создания СЗИ и технического (частного технического) задания на ее создание Работы, выполняемые на предпроектном этапе:
устанавливается необходимость обработки (обсуждения)
информации на данном объекте информатизации или защищенном помещении (ЗП);
определяется перечень сведений конфиденциального характера, подлежащих защите;
определяются (уточняются) угрозы безопасности информации и
модель вероятного нарушителя применительно к конкретным условиям функционирования объекта;
определяются условия расположения объекта информатизации относительно границ контролируемой зоны (КЗ);
определяются конфигурация и топология ОТСС в целом и их
отдельных компонентов, физические, функциональные и технологические связи ОТСС с другими системами различного уровня и назначения;
определяются конкретные технические средства и системы,
предполагаемые к использованию в разрабатываемой автоматизированной системе ; условия их расположения, их программные средства;
определяются режимы обработки информации в автоматизированной системы в целом и в отдельных компонентах;

−определяется класс защищенности автоматизированной системы; определяется степень участия персонала в информации, характер их взаимодействия между собой и со службой безопасности;
определяются мероприятия по обеспечению конфиденциальности информации на этапе проектирования объекта информатизации.
По результатам предпроектного обследования разрабатывается аналитическое обоснование необходимости создания СЗИ и задаются конкретные требования по защите информации, включаемые в техническое (частное техническое) задание на разработку СЗИ.
2. Проектирование (разработки проектов) систем защиты информации
Работы, выполняемые при проектировании:
разработка задания и проекта на строительные, строительно-монтажные работы (или реконструкцию) объекта информатизации;
−разработка раздела технического проекта на объект информатизации части реализации мероприятий по защите информации;
строительно-монтажные работы, размещение и монтаж технических средств и систем;
разработка организационно-технических мероприятий по защите информации в соответствии с предъявляемыми требованиями;
закупка сертифицированных образцов серийно выпускаемых защищенных технических средств, либо их сертификация;

закупка сертифицированных технических, программных и программно - технических средств защиты информации и их установка;
разработка (доработка) или закупка и последующая сертификация по требованиям безопасности информации программных средств защиты информации (в случае необходимости);
организация охраны и физической защиты помещений объекта информатизации разработка разрешительной системы доступа пользователей и эксплуатационного персонала к защищаемой информации;

определение и обучение подразделений и лиц, ответственных за эксплуатацию средств защиты информации;
разработка эксплуатационной документации на объект информатизации, средства защиты информации, и организационно-распорядительной документации по ЗИ.
Результатом проектирования является разработка технического проекта, эксплуатационной документации на ОИ, СЗИ, организационно-распорядительной документации по ЗИ.
Ввод в действие СЗИ
При вводе в эксплуатацию выполняются следующие мероприятия:
опытная эксплуатация средств защиты информации с другими техническими и программными средствами для проверки их
работоспособности в комплексе и отработки технологического процесса обработки (передачи) информации;
приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации.
При этом разрабатываются и передаются заказчику следующие документы :
− Приемо-сдаточный акт, подписываемый разработчиком (поставщиком) и заказчиком;

Акты внедрения средств защиты информации по результатам их приемо - сдаточных испытаний;
Приказ (указание, решение) о назначении лиц, ответственных за эксплуатацию объекта информатизации;
Приказ (указание, решение) о разрешении обработки в АС (ЗП) информации ограниченного доступа.

Основные организационно-технических мероприятия по защите информации

Основными организационно-техническими мероприятиями, которые проводятся государственной системой защиты информации, следует считать:
государственное лицензирование деятельности предприятий в области защиты информации;
аттестация объектов информации по требованиям безопасности

информации, предназначенная для оценки подготовленности систем и средств информатизации и связи к обработке информации, содержащей государственную, служебную или коммерческую тайну;
−сертификация систем защиты информации;
·категорирование предприятий, выделенных помещений и объектов вычислительной техники по степени важности обрабатываемой информации.
Последовательность и содержание организации комплексной защиты информации представлена на рис. 1.
К организационно-техническим мероприятиям, проводимым государственной системой защиты информации, также относятся:
введение территориальных, частотных, энергетических,

пространственных и временных ограничений в режимах эксплуатации технических средств, подлежащих защите;

создание и применение информационных и автоматизированных систем управления в защищенном исполнении;

разработка и внедрение технических решений и элементов защиты информации при создании вооружения и военной техники и при проектировании, строительстве и эксплуатации объектов информатизации, систем и средств автоматизации и связи.

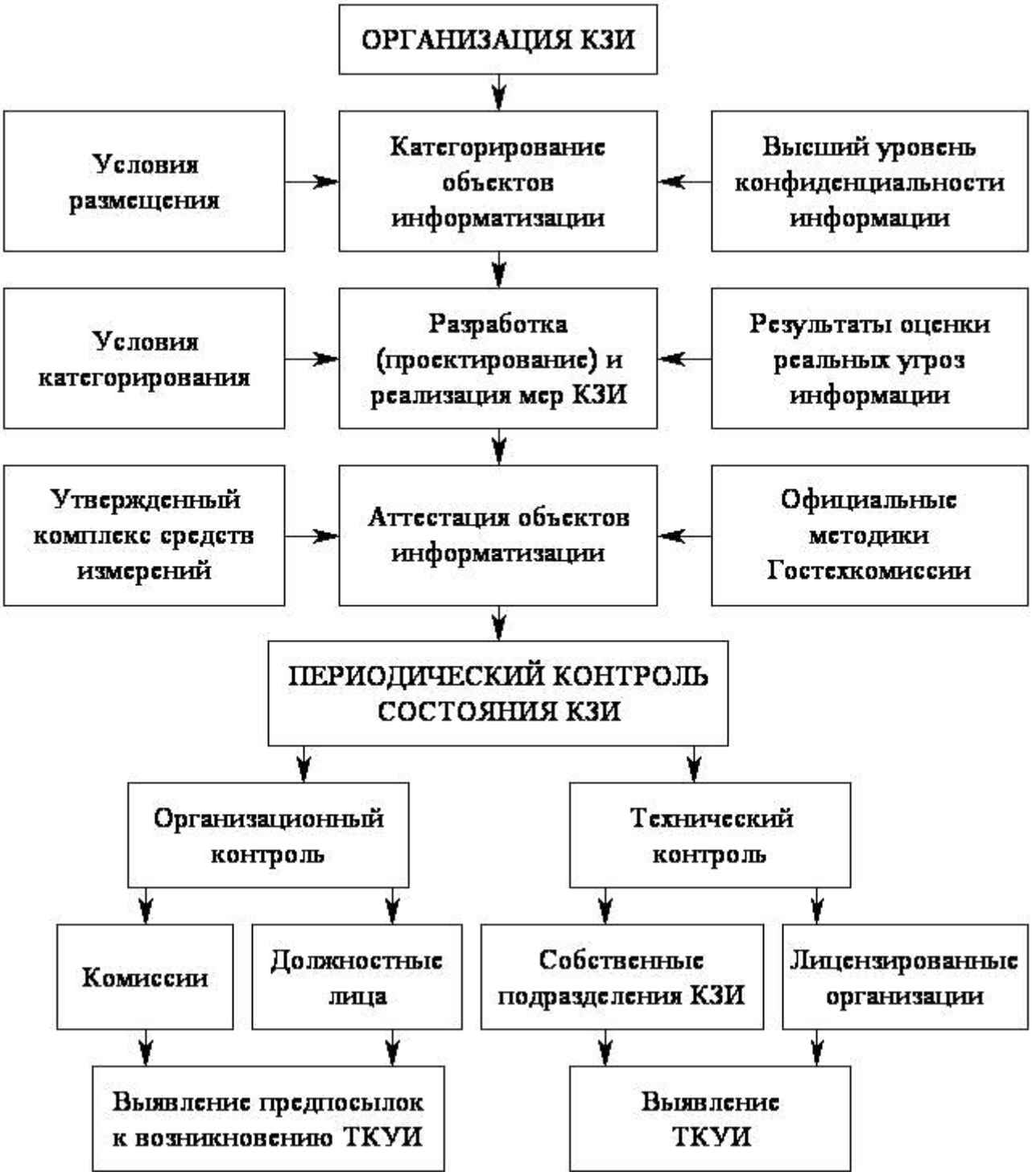


Рис. 1. Примерная схема контроля защиты информации

Мероприятия по обеспечению защиты информации.

Защита от утечки конфиденциальной информации сводится к выявлению, учету и контролю возможных каналов утечки в конкретных условиях и к проведению организационных, организационно-технических и технических мероприятий по их ликвидации.

Защита от несанкционированного доступа к конфиденциальной информации обеспечивается путем выявления, анализа и контроля

Комплексность
возможных способов несанкционированного доступа и проникновения к источникам конфиденциальной информации и реализацией организационных, организационно-технических и технических мероприятий по противодействию нсд.

Организационная защита информации - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией, и включает в себя организацию режима охраны, организацию работы с сотрудниками, с документами, организацию использования технических средств и работу по

анализу угроз информационной безопасности.
Обеспечение защиты средств обработки информации и автоматизированных рабочих мест от несанкционированного доступа достигается системой разграничения доступа субъектов к объектам. Данная система реализуется в программно-технических комплексах, в рамках операционной системы, систем управления базами данных или прикладных программ, в средствах реализации ЛВС, в использовании криптографических преобразований, методов контроля доступа.

Защита информации организационными средствами предполагает защиту без использования технических средств. Иногда, задача решается простым удалением ОТСС от границы контролируемой зоны на максимально возможное расстояние. Так же возможен вариант размещения, например, трансформаторной подстанции и контура заземления в пределах контролируемой зоны. К организационно-техническим можно отнести так же удаление ВТСС, линии которых выходят за пределы контролируемой зоны, запрещение использования ОТСС с паразитной генерацией для обработки информации, проведение специальных проверок технических средств на отсутствие закладочных устройств. Необходимо помнить, что организационно-технические меры требуют выполнение комплекса мер, предписанных нормативными документами.

При разработке СЗИ так же следует принимать во внимание то, что вся система состоит из более мелких систем. К ним относится подсистема

управления доступом, подсистема регистрации и учета, криптографическая защита информации и подсистема обеспечения целостности.

Общие принципы организации защиты конфиденциальной информации, применяемые при разработке СЗИ:

- Непрерывность
- точность

Согласованность

Эффективность

Для реализации мер защиты конфиденциальной информации должны применяться сертифицированные в установленном порядке технические средства защиты информации.

К мерам противодействия угрозам безопасности относят правовые, морально-этические, технологические, физические и технические. Морально-этические меры побуждают к созданию правовых мер (примером может быть неприязнь того, что кто-либо незнакомый Вам, может узнать Ваши фамилию имя и отчество, состояние здоровья или иную информацию личного характера). В свою очередь правовые меры побуждают к реализации организационных мер (разработка необходимых норм и правил при собирании, обработке, передаче и хранении информации), которые связаны с физическими и техническими мерами (технические средства защиты информации, физические барьеры на пути злоумышленника и т.д.).

Система безопасности - это организованная совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия, государства от внутренних и внешних угроз, в задачи которой входит разработка и осуществление мер по защите информации, формирование, обеспечение и продвижение средств обеспечения безопасности и восстановление объектов защиты, пострадавших в результате каких-либо противоправных действий.

Все эти задачи помогают в достижении целей своевременного выявления угроз, оперативного предотвращения, нейтрализации или пресечения, локализации угроз, отражения атак и уничтожении угроз.

Организационные мероприятия - это мероприятия ограничительного характера, сводящиеся основном, к регламентации доступа и использования технических средств обработки информации. Они, как правило, проводятся силами самой организации путем использования простейших организационных мер.

В общем плане организационные мероприятия предусматривают проведение следующих действий:
определение границ охраняемой зоны (территории): Охраняемая зона - это и есть кабинет директора (в моѐм варианте). Сама комната описана

пункте 1. данной работы;
определение технических средств, используемых для обработки конфиденциальной информации в пределах контролируемой территории: используются такие ТС как телефон, компьютер;

определение "опасных", с точки зрения возможности образования каналов утечки информации, технических средств и конструктивных особенностей зданий и сооружений: данный вопрос описан в пункте 2.. Основными каналами утечки информации на данном объекте являются: телефонные линии связи, акустический канал, ПЭМИН, цепи заземления;
выявление возможных путей проникновения к источникам конфиденциальной информации со стороны злоумышленников: данный вопрос описан в пункте 3.;

реализация мер по обнаружению, выявлению и контролю за обеспечением защиты информации всеми доступными средствами: данный вопрос описан в пункте 4..
Организационные мероприятия выражаются в тех или иных ограничительных мерах. Можно выделить такие ограничительные меры, как территориальные, пространственные и временные.
Территориальные ограничения сводятся к умелому расположению источников на местности или в зданиях и помещениях, исключающих подслушивание переговоров или перехват сигналов радиоэлектронных средств.
Пространственные ограничения выражаются в выборе направлений излучения тех или иных сигналов в сторону наименьшей возможности их перехвата злоумышленниками.
Временные ограничения проявляются в сокращении до минимума времени работы технических средств, использовании скрытых методов связи, шифровании и других мерах защиты.
Одной из важнейших задач организационной деятельности является определение состояния технической безопасности объекта, его помещений, подготовка и выполнение организационных мер, исключающих возможность неправомерного овладения конфиденциальной информацией, воспрещение ее разглашения, утечки и несанкционированного доступа к охраняемым секретам.
Организационно-технические мероприятия обеспечивают блокирование разглашения и утечки конфиденциальных сведений через технические средства обеспечения производственной и трудовой деятельности, а также противодействие техническим средствам промышленного шпионажа с помощью специальных технических средств, устанавливаемых на элементы конструкций зданий, помещений и технических средств, потенциально

образующих каналы утечки информации. В этих целях возможно использование:

технических средств пассивной защиты, например фильтров, ограничителей и тому подобных средств развязки акустических,

электрических и электромагнитных систем защиты сетей телефонной связи, энергоснабжения, радио- и часофикации и др.;
− технических средств активной защиты: датчиков акустических шумов и электромагнитных помех.
Организационно-технические мероприятия по защите информации можно подразделить на пространственные, режимные и энергетические.
Пространственные меры выражаются в уменьшении ширины диаграммы направленности, ослаблении боковых и заднего лепестков диаграммы направленности излучения радиоэлектронных средств (РЭС).
Режимные меры сводятся к использованию скрытых методов передачи информации по средствам связи: шифрование, квазипеременные частоты передачи и др.
Энергетические - это снижение интенсивности излучения и работа РЭС на пониженных мощностях.
Технические мероприятия - это мероприятия, обеспечивающие приобретение, установку и использование в процессе производственной деятельности специальных, защищенных от побочных излучений (безопасных) технических средств или средств, ПЭМИН которых не превышают границу охраняемой территории.
Технические мероприятия по защите конфиденциальной информации можно подразделить на скрытие, подавление и дезинформацию.
Скрытие выражается в использовании радиомолчания и создании пассивных помех приемным средствам злоумышленников.
Подавление - это создание активных помех средствам злоумышленников .
Дезинформация - это организация ложной работы технических средств связи и обработки информации; изменение режимов использования частот и регламентов связи; показ ложных демаскирующих признаков деятельности и опознавания .
Защитные меры технического характера могут быть направлены на конкретное техническое устройство или конкретную аппаратуру и выражаются в таких мерах, как отключение аппаратуры на время ведения конфиденциальных переговоров или использование тех или иных защитных устройств типа ограничителей, буферных средств, фильтров и устройств зашумления .

Можно так классифицировать потенциальные угрозы, против которых направлены технические меры защиты информации:
Потери информации из-за сбоев оборудования:
−перебои электропитания;

сбои дисковых систем;

−сбои работы серверов, рабочих станций, сетевых карт и т.д.
Потери информации из-за некорректной работы программ:
−потеря или изменение данных при ошибках ПО;
−потери при заражении системы компьютерными вирусами;
Потери, связанные с несанкционированным доступом:
несанкционированное копирование, уничтожение или подделка информации ;
−ознакомление с конфиденциальной информацией.
Ошибки обслуживающего персонала и пользователей:
−случайное уничтожение или изменение данных;

некорректное использование программного и аппаратного обеспечения , ведущее к уничтожению или изменению данных.
Сами технические меры защиты можно разделить на:
средства аппаратной защиты, включающие средства защиты кабельн ой системы, систем электропитания, и т.д.
программные средства защиты, в том числе: криптография,

антивирусные программы, системы разграничения полномочий, средства контроля доступа и т.д.
административные меры защиты, включающие подготовку и

обучение персонала, организацию тестирования и приема в эксплуатацию программ , контроль доступа в помещения и т.д.
Следует отметить, что подобное деление достаточно условно, поскольку современные технологии развиваются в направлении сочетания программных и аппаратных средств защиты. Наибольшее распространение такие программно-аппаратные средства получили, в частности, в области контроля доступа, защиты от вирусов и т.д.

Практическое задание
Выделите информацию, не подлежащую защите согласно нормативно-правовым актам, и выполнить проектирование организационных и технических мер по защите этой информации.
Выполните построение комплексной системы организационных мер для выбранного предприятия.

Контрольные вопросы

Что понимается под информационной безопасностью?

Назовите основные способы защиты информации.

Назовите способы несанкционированного получения конфиденциальной информации.

Какие задачи решаются в ходе разработки и внедрения КСЗИ? Назовите этапы создания системы защиты.

Лабораторная работа 12.
Изучение методов построения комплексной защиты сетевой файловой системы

Цель работы: изучить методы построения защищѐнной сетевой файловой системы.

Теоретическая часть

Файловые серверы и распределенные системы

Ключевым компонентом любой распределенной системы является файловая система, которая также является распределенной. С программной точки зрения распределенная файловая система является сетевой службой. Файловая служба включает программы-серверы и программы-клиенты, взаимодействующие с помощью определенного протокола по сети между собой.

Таким образом, файловым сервером называют не только компьютер, на котором хранятся предоставляемые в совместный доступ файлы, но и программу (или процесс, в рамках которого выполняется данная программа), которая работает на этом компьютере и обеспечивает совокупность услуг по доступу к файлам и каталогам на удаленном компьютере. Соответственно программу, работающую на клиентском компьютере и обращающуюся к файловому серверу с запросами, называют клиентом файловой системы, как компьютер, на котором она работает. Такая неоднозначность терминов «файловый сервер» и «клиент» обычно не вызывает затруднений, так как из контекста, как правило, понятно, о каком программном или аппаратном компоненте сети идет речь.

сети может одновременно работать несколько программных файловых серверов, каждый из которых предлагает различные файловые услуги. Например, в распределенной системе могут быть два сервера, которые предоставляют файловые услуги систем UNIX и Windows соответственно, и пользовательские процессы могут обращаться к подходящему серверу.

Кроме того, один компьютер может в одно и то же время предоставлять пользователям сети услуги различных файловых служб, для этого нужно, чтобы на этом компьютере работало несколько процессов, каждый из которых реализовывал бы файловую службу определенного типа.
Файловая служба в распределенных файловых системах (впрочем, как в централизованных) имеет две функционально различные части: собственно файловую службу и службу каталогов файловой системы. Первая имеет дело с операциями над отдельными файлами, такими как чтение, запись или добавление, а вторая – с созданием каталогов и управлением ими, добавлением и удалением файлов из каталогов и т. п.
В хорошо организованной распределенной системе пользователи не знают, как реализована файловая система. В частности, они не знают количество файловых серверов, их месторасположение и функции. Они только знают, что если процедура определена в файловой службе, то требуемая работа каким-то образом выполняется, возвращая им результаты. Более того, пользователи даже не должны знать, что файловая система является распределенной. В идеале для пользователя она должна выглядеть так же, как и централизованная файловая система.

Структура сетевой файловой системы

ФС в общем случае включает следующие элементы:
- локальная файловая система;
- интерфейс локальной файловой системы;
- сервер сетевой файловой системы;
- клиент сетевой файловой системы;
- интерфейс сетевой файловой системы; - протокол клиент-сервер сетевой файловой системы.

Клиенты сетевой ФС – это программы, которые работают на многочисленных компьютерах, подключенных к сети. Эти программы обслуживают запросы приложений на доступ к файлам, хранящимся на

удаленном компьютере. В качестве таких приложений часто выступают графические или символьные оболочки ОС, такие как Windows Explorer или UNIX shell, а также любые другие пользовательские программы.
Клиент сетевой ФС передает по сети запросы другому программному компоненту – серверу сетевой ФС, работающему на удаленном компьютере. Сервер, получив запрос, может выполнить его либо самостоятельно, либо, что является более распространенным вариантом, передать запрос локальной файловой системе для отработки. После получения ответа от локальной файловой системы сервер передает его по сети клиенту, а тот, в свою очередь, –приложению, обратившемуся с запросом.
Приложения обращаются к клиенту сетевой ФС, используя определенный программный интерфейс, который в данном случае является интерфейсом сетевой файловой системы. Этот интерфейс стараются сделать как можно более похожим на интерфейс локальной файловой системы, чтобы соблюсти принцип прозрачности. При полном совпадении интерфейсов приложение может обращаться к локальным и удаленным файлам и каталогам с помощью одних и тех же системных вызовов, совершенно не принимая во внимание места хранения данных. Например, если на серверах сети используются локальные файловые системы FAT, то интерфейс сетевой файловой системы повторяет системные вызовы FAT.
Клиент и сервер сетевой файловой системы взаимодействуют друг с другом по сети по определенному протоколу. В случае совпадения интерфейсов локальной и сетевой файловых систем этот протокол может быть достаточно простым – в его функции будет входить ретрансляция серверу запросов, принятых клиентом от приложений, с которыми тот затем будет обращаться к локальной файловой системе. Одним из механизмов, используемых для этой цели, может быть механизм RPC.

Шифрование

Шифрование – это краеугольный камень всех служб информационной безопасности, будь то система аутентификации или авторизации, средства создания защищенного канала или способ безопасного хранения данных. Любая процедура шифрования, превращающая информацию из обычного «понятного» вида в «нечитабельный» зашифрованный вид, естественно, должна быть дополнена процедурой дешифрирования, которая, будучи примененной к зашифрованному тексту, снова приводит его в понятный вид. Пара процедур – шифрование и дешифрирование – называется криптосистемой.

Информацию, над которой выполняются функции шифрования и дешифрирования, будем условно называть «текст», учитывая, что это может быть также числовой массив или графические данные.

В современных алгоритмах шифрования предусматривается Наличие параметра – секретного ключа. В криптографии принято правило Керкхоффа: «Стойкость шифра должна определяться только секретностью ключа». Так, все стандартные алгоритмы шифрования (например, DES, PGP) широко известны, их детальное описание содержится в легко доступных документах, но от этого их эффективность не снижается. Злоумышленнику может быть все известно об алгоритме шифрования, кроме секретного ключа (следует отметить, однако, что существует немало фирменных алгоритмов, описание которых не публикуется).

Алгоритм шифрования считается раскрытым, если найдена процедура, позволяющая подобрать ключ за реальное время. Сложность алгоритма раскрытия является одной из важных характеристик криптосистемы и называется криптостойкостью.

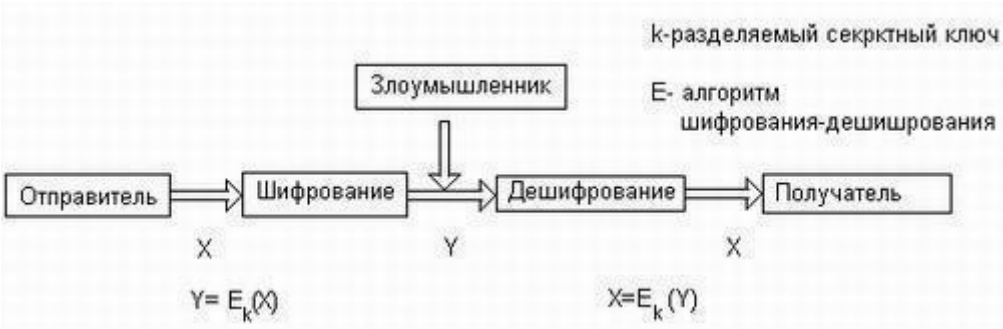
Существуют два класса криптосистем – симметричные и асимметричные. В симметричных схемах шифрования (классическая криптография) секретный ключ зашифровки совпадает с секретным ключом расшифровки. В асимметричных схемах шифрования (криптография с

открытым ключом) открытый ключ зашифровки не совпадает с секретным ключом расшифровки.

Симметричные алгоритмы шифрования

На рисунке 1 приведена классическая модель симметричной криптосистемы, теоретические основы которой впервые были изложены в 1949 году в работе Клода Шеннона. В данной модели три участника: отправитель, получатель, злоумышленник. Задача отправителя заключается в том, чтобы по открытому каналу передать некоторое сообщение в защищенном виде. Для этого он на ключе k зашифровывает открытый текст X и передает шифрованный текст Y. Задача получателя заключается в том, чтобы расшифровать Y и прочитать сообщение X. Предполагается, что отправитель имеет свой источник ключа. Сгенерированный ключ заранее по надежному каналу передается получателю. Задача злоумышленника заключается в перехвате и чтении передаваемых сообщений, а также в имитации ложных сообщений.
Рисунок 1 – Модель симметричного шифрования

Модель является универсальной – если зашифрованные; данные хранятся в компьютере и никуда не передаются, отправитель и получатель совмещаются в одном лице, а в роли злоумышленника выступает некто, имеющий доступ к



компьютеру в ваше отсутствие.

Несимметричные алгоритмы шифрования

В середине 70-х двое ученых – Винфилд Диффи и Мартин Хеллман – описали принципы шифрования с открытыми ключами.

Особенность шифрования на основе открытых ключей состоит в том, что одновременно генерируется уникальная пара ключей, таких, что текст, зашифрованный одним ключом, может быть расшифрован только с использованием второго ключа и наоборот.

В модели криптосхемы с открытым ключом также три участника: отправитель, получатель, злоумышленник (рисунок 2). Задача отправителя заключается в том, чтобы по открытому каналу связи передать некоторое сообщение в защищенном виде. Получатель генерирует на своей стороне два ключа: открытый E и закрытый D. Закрытый ключ D (часто называемый также личным ключом) абонент должен сохранять в защищенном месте, а открытый ключ E он может передать всем, с кем он хочет поддерживать защищенные отношения. Открытый ключ используется для шифрования текста, но расшифровать текст можно только с помощью закрытого ключа. Поэтому открытый ключ передается отправителю в незащищенном виде. Отправитель, используя открытый ключ получателя, шифрует сообщение X и передает его получателю. Получатель расшифровывает сообщение своим закрытым ключом D.

Очевидно, что числа, одно из которых используется для шифрования текста, а другое – для дешифрирования, не могут быть независимыми друг от друга, а значит, есть теоретическая возможность вычисления закрытого ключа по открытому, но это связано с огромным количеством вычислений, которые требуют соответственно огромного времени. Поясним принципиальную связь между закрытым и открытым ключами следующей аналогией.

Рисунок 2 – Модель криптосхемы с открытым ключом

Пусть абонент 1 (рисунок 3, а) решает вести секретную переписку со своими сотрудниками на малоизвестном языке, например санскрите. Для этого он обзаводится санскритско-русским словарем, а всем своим абонентам посылает русско-санскритские словари. Каждый из них, пользуясь словарем, пишет сообщения на санскрите и посылает их абоненту 1, который переводит их на русский язык, пользуясь доступным только ему санскритско-русским словарем. Очевидно, что здесь роль открытого ключа E играет русско-санскритский словарь, а роль закрытого ключа D – санскритско-русский словарь. Могут ли абоненты 2, 3 и 4 прочитать чужие сообщения S_2, S_3, S_4, которые посылает каждый из них абоненту 1? Вообще-то нет, так как, для этого им нужен санскритско-русский словарь, обладателем которого является только абонент 1. Но теоретическая возможность этого имеется, так как затратив массу времени, можно прямым перебором составить санскритско-русский словарь по русско-санскритскому словарю. Такая процедура, требующая больших временных затрат, является отдаленной аналогией восстановления закрытого ключа по открытому.

На рисунке 3, б показана другая схема использования открытого и закрытого ключей, целью которой является подтверждение авторства (аутентификация или электронная подпись) посылаемого сообщения. В этом случае поток сообщений имеет обратное направление – от абонента 1, обладателя закрытого ключа D, к его корреспондентам, обладателям открытого ключа E. Если абонент 1 хочет аутентифицировать себя (поставить электронную подпись), то он шифрует известный текст своим закрытым ключом D и передает шифровку своим корреспондентам. Если им удается расшифровать текст открытым ключом абонента 1, то это доказывает, что текст был

зашифрован его же закрытым ключом, а значит, именно он является автором этого сообщения. Заметим, что в этом случае
сообщения S_2, S_3, 84, адресованные разным абонентам, не являются секретными, так как все они – обладатели одного и того же открытого ключа, с помощью которого они могут расшифровывать все сообщения, поступающие от абонента 1.
Если же нужна взаимная аутентификация и двунаправленный секретный обмен сообщениями, то каждая из общающихся сторон генерирует собственную пару ключей и посылает открытый ключ своему корреспонденту.
Для того чтобы в сети все п абонентов имели возможность не только принимать зашифрованные сообщения, но и сами посылать таковые, каждый абонент должен обладать своей собственной парой ключей E и D. Всего в сети будет 2п ключей: п открытых ключей для шифрования и n секретных ключей для дешифрирования. Таким образом решается проблема масштабируемости — квадратичная зависимость количества ключей от числа абонентов в симметричных алгоритмах заменяется линейной зависимостью в несимметричных алгоритмах. Исчезает и задача секретной доставки ключа. Злоумышленнику нет смысла стремиться завладеть открытым ключом, поскольку это не дает возможности расшифровывать текст или вычислить закрытый ключ.

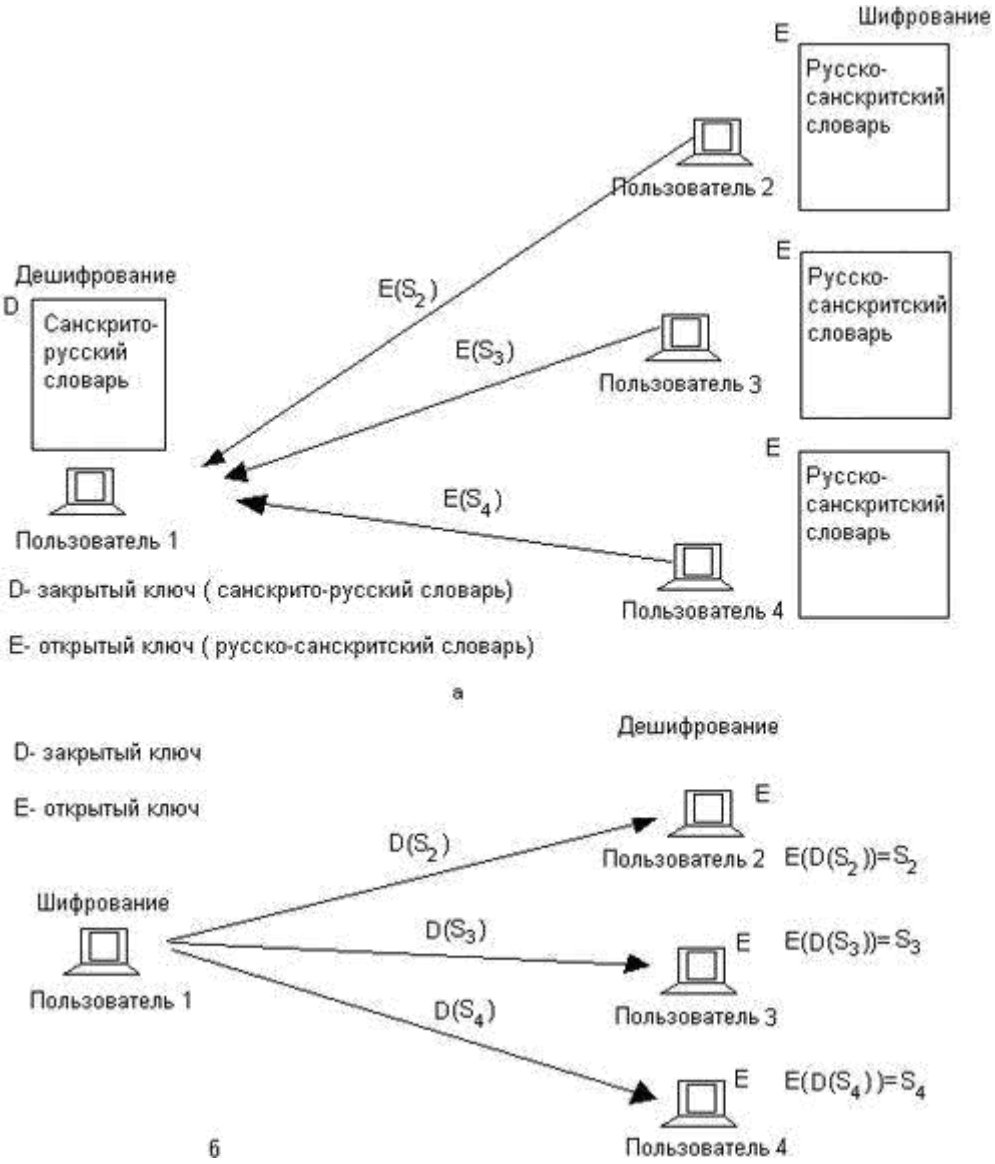


Рисунок 3 – Две схемы использования открытого и закрытого ключей

Хотя информация об открытом ключе не является секретной, ее нужно защищать от подлогов, чтобы злоумышленник под именем легального пользователя не навязал свой открытый ключ, после чего с помощью своего закрытого ключа он может расшифровывать все сообщения, посылаемые легальному пользователю и отправлять свои сообщения от его имени. Проще всего было бы распространять списки, связывающие имена пользователей с их открытыми ключами широковещательно, путем публикаций в средствах массовой информации (бюллетени, специализированные журналы и т. п.). Однако при таком подходе мы снова, как и в случае с паролями,

сталкиваемся с плохой масштабируемостью. Решением этой проблемы является технология цифровых сертификатов. Сертификат – это электронный документ, который связывает конкретного пользователя с конкретным ключом.

Аутентификация

Аутентификация (authentication) предотвращает доступ к сети нежелательных лиц и разрешает вход для легальных пользователей. Термин «аутентификация» в переводе с латинского означает «установление подлинности». Аутентификацию следует отличать от идентификации. Идентификаторы пользователей используются в системе с теми же целями, что и идентификаторы любых других объектов, файлов, процессов, структур данных, но они не связаны непосредственно с обеспечением безопасности. Идентификация заключается в сообщении пользователем системе своего идентификатора, в то время как аутентификация – это процедура доказательства пользователем того, что он есть тот, за кого себя выдает, в частности, доказательство того, что именно ему принадлежит введенный им идентификатор.

В процедуре аутентификации участвуют две стороны: одна сторона доказывает свою аутентичность, предъявляя некоторые доказательства, а другая сторона – аутентификатор – проверяет эти доказательства и принимает решение. В качестве доказательства аутентичности используются самые разнообразные приемы:

аутентифицируемый может продемонстрировать знание некоего общего для обеих сторон секрета: слова (пароля) или факта (даты и места события , прозвища человека и т. п.);

аутентифицируемый может продемонстрировать, что он владеет неким уникальным предметом (физическим ключом), в качестве которого может выступать, например, электронная магнитная карта;

аутентифицируемый может доказать свою идентичность, используя собственные биохарактеристики: рисунок радужной оболочки глаза или

отпечатки пальцев, которые предварительно были занесены в базу данных аутентификатора .

Сетевые службы аутентификации строятся на основе всех этих приемов, но чаще всего для доказательства идентичности пользователя используются пароли. Простота и логическая ясность механизмов аутентификации на основе паролей в какой-то степени компенсирует известные слабости паролей. Это, во-первых, возможность раскрытия и разгадывания паролей, а во-вторых, возможность «подслушивания» пароля путем анализа сетевого трафика. Для снижения уровня угрозы от раскрытия паролей администраторы сети, как правило, применяют встроенные программные средства для формирования политики назначения и использования паролей: задание максимального и минимального сроков действия пароля, хранение списка уже использованных паролей, управление поведением системы после нескольких неудачных попыток логического
входа и т. п. Перехват паролей по сети можно предупредить путем их шифрования перед передачей в сеть.

Легальность пользователя может устанавливаться по отношению к различным системам. Так, работая в сети, пользователь может проходить процедуру аутентификации и как локальный пользователь, который претендует на использование ресурсов только данного компьютера, и как пользователь сети, который хочет получить доступ ко всем сетевым ресурсам. При локальной аутентификации пользователь вводит свои идентификатор и пароль, которые автономно обрабатываются операционной системой, установленной на данном компьютере. При логическом входе в сеть данные о пользователе (идентификатор и пароль) передаются на сервер, который хранит учетные записи обо всех пользователях сети. Многие приложения имеют свои средства определения, является ли пользователь законным. И тогда пользователю приходится проходить дополнительные этапы проверки.

качестве объектов, требующих аутентификации, могут выступать не только пользователи, но и различные устройства, приложения, текстовая и другая информация. Так, например, пользователь, обращающийся с запросом корпоративному серверу, должен доказать ему свою легальность, но он также должен убедиться сам, что ведет диалог действительно с сервером своего предприятия. Другими словами, сервер и клиент должны пройти процедуру взаимной аутентификации'. Здесь мы имеем дело с аутентификацией на уровне приложений. При установлении сеанса связи между двумя устройствами также часто предусматриваются процедуры взаимной аутентификации на более низком, канальном уровне. Примером такой процедуры является аутентификация по протоколам PAP и CHAP, входящим в семейство протоколов PPP. Аутентификация данных означает доказательство целостности этих данных, а также того, что они поступили именно от того человека, который объявил об этом. Для этого используется механизм электронной подписи.

вычислительных сетях процедуры аутентификации часто реализуются теми же программными средствами, что и процедуры авторизации. В отличие от аутентификации, которая распознает легальных и нелегальных пользователей, система авторизации имеет дело только с легальными пользователями, которые уже успешно прошли процедуру аутентификации. Цель подсистем авторизации состоит в том, чтобы предоставить каждому легальному пользователю именно те виды доступа и к тем ресурсам, которые были для него определены администратором системы.

Авторизация доступа

Средства авторизации (authorization) контролируют доступ легальных пользователей к ресурсам системы, предоставляя каждому из них именно те права, которые ему были определены администратором. Кроме предоставления прав доступа пользователям к каталогам, файлам и принтерам система авторизации может контролировать возможность выполнения пользователями различных системных функций, таких как локальный доступ к серверу, установка системного времени, создание резервных копий данных, выключение сервера и т. п.

Система авторизации наделяет пользователя сети правами выполнять определенные действия над определенными ресурсами. Для этого могут быть использованы различные формы предоставления правил доступа, которые часто делят на два класса:

− избирательный доступ;

− мандатный доступ.

Избирательные права доступа реализуются в операционных системах универсального назначения. В наиболее распространенном варианте такого подхода определенные операции над определенным ресурсом разрешаются или запрещаются пользователям или группам пользователей, явно указанным своими идентификаторами. Например, пользователю, имеющему идентификатор User_T, может быть разрешено выполнять операции чтения и записи по отношению к файлу Filet. Модификацией этого способа является использование для идентификации пользователей их должностей, или факта их принадлежности к персоналу того или иного производственного подразделения, или еще каких-либо других позиционирующих характеристик. Примером такого правила может служить следующее: файл бухгалтерской отчетности BUCH могут читать работники бухгалтерии и руководитель предприятия.

Мандатный подход к определению прав доступа заключается в том, что вся информация делится на уровни в зависимости от степени секретности, а все

пользователи сети также делятся на группы, образующие иерархию в соответствии с уровнем допуска к этой информации. Такой подход используется в известном делении информации на информацию для служебного пользования, «секретно», «совершенно секретно». При этом пользователи этой информации в зависимости от определенного для них статуса получают различные формы допуска: первую, вторую или третью. В отличие от систем с избирательными правами доступа в системах с мандатным подходом пользователи в принципе не имеют возможности изменить уровень доступности информации. Например, пользователь более высокого уровня не может разрешить читать данные из своего файла пользователю, относящемуся к более низкому уровню. Отсюда видно, что мандатный подход является более строгим, он в корне пресекает всякий волюнтаризм со стороны пользователя. Именно поэтому он часто используется в системах военного назначения.

Процедуры авторизации реализуются программными средствами, которые могут быть встроены в операционную систему или в приложение, а также могут поставляться в виде отдельных программных продуктов. При этом программные системы авторизации могут строиться на базе двух схем:

- централизованная схема авторизации, базирующаяся на сервере;
- децентрализованная схема, базирующаяся на рабочих станциях.

первой схеме сервер управляет процессом предоставления ресурсов пользователю. Главная цель таких систем — реализовать «принцип единого входа». В соответствии с централизованной схемой пользователь один раз логически входит в сеть и получает на все время работы некоторый набор разрешений по доступу к ресурсам сети. Система Kerberos с ее сервером безопасности и архитектурой клиент-сервер является наиболее известной системой этого типа. Системы TACACS и RADIUS, часто применяемые совместно с системами удаленного доступа, также реализуют этот подход.

При втором подходе рабочая станция сама является защищенной – средства защиты работают на каждой машине, и сервер не требуется. Рассмотрим

работу системы, в которой не предусмотрена процедура однократного логического входа. Теоретически доступ к каждому приложению должен контролироваться средствами безопасности самого приложения или же средствами, существующими в той операционной среде, в которой оно работает. В корпоративной сети администратору придется отслеживать работу механизмов безопасности, используемых всеми типами приложений – электронной почтой, службой каталогов локальной сети, базами данных хостов и т. п. Когда администратору приходится добавлять или удалять пользователей, то часто требуется вручную конфигурировать доступ к каждой программе или системе.

В крупных сетях часто применяется комбинированный подход предоставления пользователю прав доступа к ресурсам сети: сервер удаленного доступа ограничивает доступ пользователя к подсетям или серверам корпоративной сети, то есть к укрупненным элементам сети, а каждый отдельный сервер сети сам по себе ограничивает доступ пользователя к своим внутренним ресурсам: разделяемым каталогам, принтерам или приложениям. Сервер удаленного доступа предоставляет доступ на основании имеющегося у него списка прав доступа пользователя (Access Control List, ACL), а каждый отдельный сервер сети предоставляет доступ к своим ресурсам на основании хранящегося у него списка прав доступа, например ACL файловой системы.

Подчеркнем, что системы аутентификации и авторизации совместно выполняют одну задачу, поэтому необходимо предъявлять одинаковый уровень требований к системам авторизации и аутентификации. Ненадежность одного звена здесь не может быть компенсирована высоким качеством другого звена. Если при аутентификации используются пароли, то требуются чрезвычайные меры по их защите. Однажды украденный пароль открывает двери ко всем приложениям и данным, к которым пользователь с этим паролем имел легальный доступ.

Аудит

Аудит (auditing) – фиксация в системном журнале событий, связанных с доступом к защищаемым системным ресурсам. Подсистема аудита современных ОС позволяет дифференцирование задавать перечень интересующих администратора событий с помощью удобного графического интерфейса. Средства учета и наблюдения обеспечивают возможность обнаружить и зафиксировать важные события, связанные с безопасностью, или любые попытки создать, получить доступ или удалить системные ресурсы. Аудит используется для того, чтобы засекать даже неудачные попытки «взлома» системы.

Учет и наблюдение означает способность системы безопасности «шпионить» за выбранными объектами и их пользователями и выдавать сообщения тревоги, когда кто-нибудь пытается читать или модифицировать системный файл. Если кто-то пытается выполнить действия, определенные системой безопасности для отслеживания, то система аудита пишет сообщение в журнал регистрации, идентифицируя пользователя. Системный менеджер может создавать отчеты о безопасности, которые содержат информацию из журнала регистрации. Для «сверхбезопасных» систем предусматриваются аудио- и видеосигналы тревоги, устанавливаемые на машинах администраторов, отвечающих за безопасность.

Поскольку никакая система безопасности не гарантирует защиту на уровне 100 %, то последним рубежом в борьбе с нарушениями оказывается система аудита.

Действительно, после того как злоумышленнику удалось провести успешную атаку, пострадавшей стороне не остается ничего другого, как обратиться к службе аудита. Если при настройке службы аудита были правильно заданы события, которые требуется отслеживать, то подробный анализ записей в журнале может дать много полезной информации. Эта информация, возможно, позволит найти злоумышленника или по крайней

мере предотвратить повторение подобных атак путем устранения уязвимых мест в системе защиты.

Технология защищенного канала

Как уже было сказано, задачу защиты данных можно разделить на две подзадачи: защиту данных внутри компьютера и защиту данных в процессе их передачи из одного компьютера в другой. Для обеспечения безопасности данных при их передаче по публичным сетям используются различные технологии защищенного канала.

Технология защищенного капала призвана обеспечивать безопасность передачи данных по открытой транспортной сети, например по Интернету. Защищенный канал подразумевает выполнение трех основных функций: взаимную аутентификацию абонентов приостановлении

соединения, которая может быть выполнена, например, путем обмена паролями ;

защиту передаваемых по каналу сообщений от несанкционированного доступа, например, путем шифрования;

подтверждение целостности поступающих по каналу сообщений, например , путем передачи одновременно с сообщением его дайджеста.

Совокупность защищенных каналов, созданных предприятием в публичной сети для объединения своих филиалов, часто называют виртуальной частной сетью (Virtual Private Network, VPN).

Существуют разные реализации технологии защищенного канала, которые, в частности, могут работать на разных уровнях модели OSI. Так, функции популярного протокола SSL соответствуют представительному уровню модели OSI. Новая версия сетевого протокола IP предусматривает все функции – взаимную аутентификацию, шифрование и обеспечение целостности , – которые по определению свойственны защищенному каналу, протокол туннелирования PPTP защищает данные на канальном уровне. зависимости от места расположения программного обеспечения защищенного канала различают две схемы его образования:

схему с конечными узлами, взаимодействующими через публичную сеть (рисунок 4, а);
схему с оборудованием поставщика услуг публичной сети, расположенным на границе между частной и публичной сетями (рисунок 4, б).

В первом случае защищенный канал образуется программными средствами, установленными на двух удаленных компьютерах, принадлежащих двум разным локальным сетям одного предприятия и связанных между собой через публичную сеть. Преимуществом этого подхода является полная защищенность канала вдоль всего пути следования, а также возможность использования любых протоколов создания защищенных каналов, лишь бы на конечных точках канала поддерживался один и тот же протокол. Недостатки заключаются в избыточности и децентрализованности решения. Избыточность состоит в том, что вряд ли стоит создавать защищенный канал на всем пути прохождения данных: уязвимыми для злоумышленников обычно являются сети с коммутацией пакетов, а не каналы телефонной сети или выделенные каналы, через которые локальные сети подключены к территориальной сети. Поэтому защиту каналов доступа к публичной сети можно считать избыточной. Децентрализация заключается в том, что для каждого компьютера, которому требуется предоставить услуги защищенного канала, необходимо отдельно устанавливать, конфигурировать и администрировать программные средства защиты данных. Подключение каждого нового компьютера к защищенному каналу требует выполнения этих трудоемких работ заново.

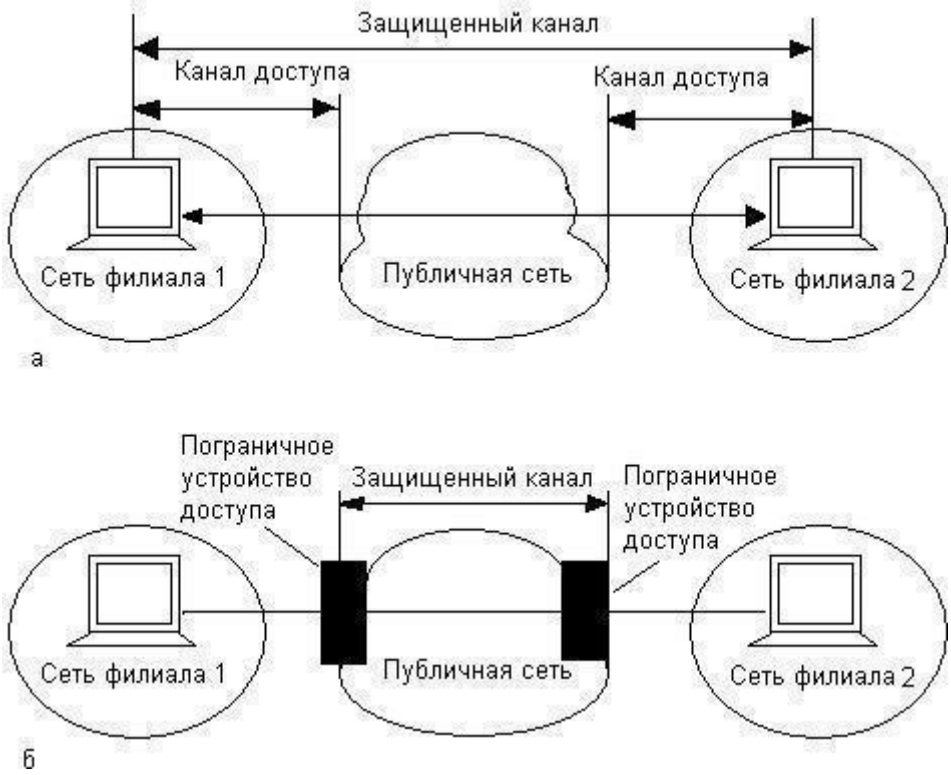


Рисунок 4 – Два способа образования защищенного канала

Во втором случае клиенты и серверы не участвуют в создании защищенного канала – он прокладывается только внутри публичной сети с коммутацией пакетов, например внутри Интернета. Канал может быть проложен, например, между сервером удаленного доступа поставщика услуг публичной сети и пограничным маршрутизатором корпоративной сети. Это хорошо масштабируемое решение, управляемое централизованно как администратором корпоративной сети, так и администратором сети поставщика услуг. Для компьютеров корпоративной сети канал прозрачен – программное обеспечение этих конечных узлов остается без изменений. Такой гибкий подход позволяет легко образовывать новые каналы защищенного взаимодействия между компьютерами независимо от их места расположения. Реализация этого подхода сложнее — нужен стандартный

протокол образования защищенного канала, требуется установка у всех поставщиков услуг программного обеспечения, поддерживающего такой протокол, необходима поддержка протокола производителями пограничного коммуникационного оборудования. Однако вариант, когда все заботы по поддержанию защищенного канала берет на себя поставщик услуг публичной сети, оставляет сомнения в надежности защиты: во-первых, незащищенными оказываются каналы доступа к публичной сети, во-вторых, потребитель услуг чувствует себя в полной зависимости от надежности поставщика услуг. И тем не менее, специалисты прогнозируют, что именно вторая схема в ближайшем будущем станет основной в построении защищенных каналов.

Практическое задание

Дайте исходную характеристику сетевой файловой системы используемой на предприятии. Предложите мероприятия по улучшению имеющейся сетевой ФС и докажите необходимость и эффективность предложенных мер.

Контрольные вопросы

Опишите структуру сетевой файловой системы
Дайте характеристику использования симметричных алгоритмы шифрования в сетевой ФС
Дайте характеристику средств аутентификации в сетевой ФС
Дайте характеристику средств авторизации доступа
Дайте характеристику средств аудита
Опишите способы построения защищенного канала связи

Лабораторная работа 13.
Комплексная защита электронной почты и документооборота
Цель работы: изучить методы комплексного построения системы защиты электронной почты и документооборота.

Теоретическая часть
Общие сведения о процедурах защиты электронной почты:
Для понимания системы мероприятий комплексной защиты электронной почты важно ясно представлять структуру объекта защиты информации и характер информационных связей и взаимодействий, лежащих в основе электронного документооборота.
Пользователь, работающий с электронной почтой, оперирует традиционными понятиями и объектами: адрес, конверт, вложения, почтовый ящик и т.д. Что такое электронное письмо? Это, прежде всего, файл. Давайте посмотрим, что скрывается за понятной всем иконкой электронного письма (рисунок 1).

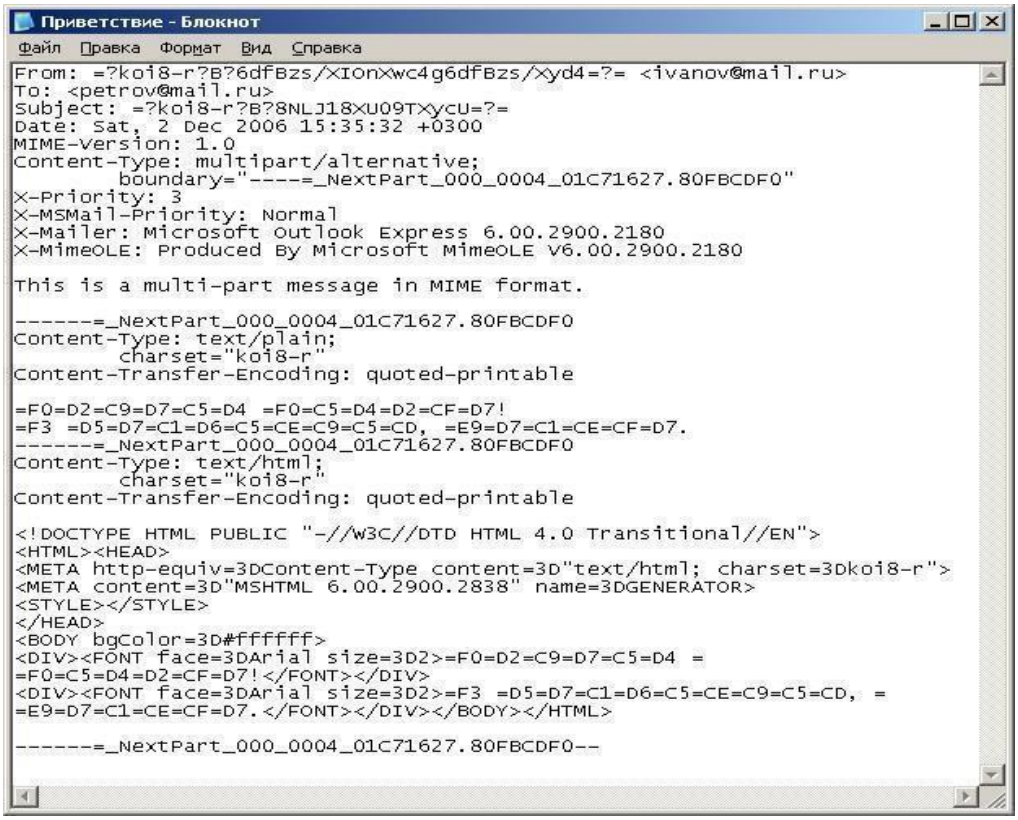


Рисунок 1 – Текстовый файл электронного письма

Перед нами обыкновенный текстовый файл. В действительности ему соответствует следующее электронное письмо (рисунок 2).

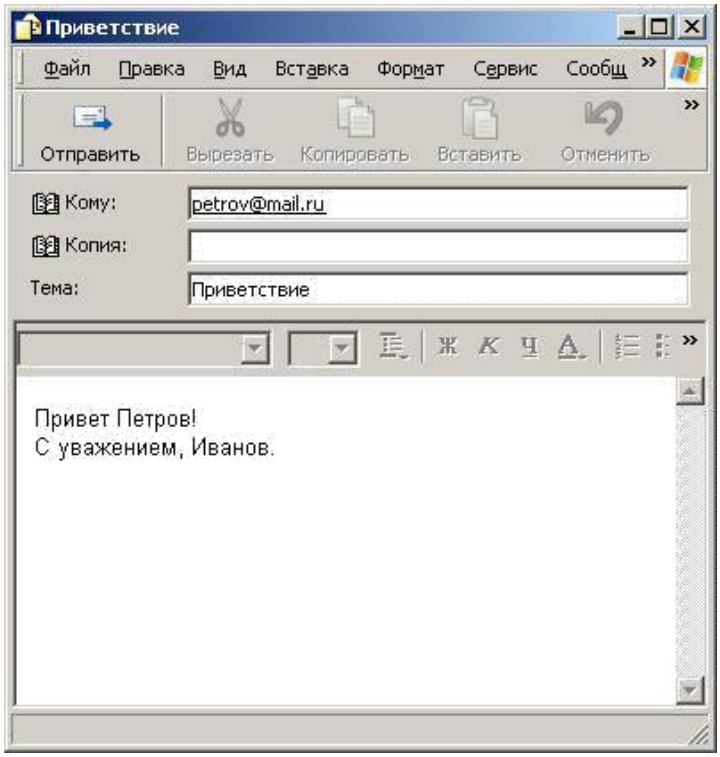


Рисунок 2 – Текст электронного письма

Из этого можно сделать вывод, что ***электронное письмо, в привычном для нас понимании, есть результат интерпретации текстового файла клиентской программой системы электронной почты.*** В действительности система электронной почты оперирует файлами. Значит, ***защита электронной почты опирается на рассмотренную ранее типовую задачу защиты сетевой файловой системы.***

В небольших компаниях система электронной почты может быть построена на основе файловой системы. Например, по такому пути пошли при реализации электронной почты в операционных системах семейства Unix. В специальной папке на сервере хранятся файлы, имена которых соответствуют пользователям системы электронной почты. Фактически ***для реализации полноценной системы электронной почты*** нам необходима программа доставки электронных сообщений в почтовые ящики, пользователь и редактор сообщений электронной почты для работы с ними.

Далее на схеме представлена структура объекта защиты информации с расположением его элементов в одной из возможных зон (рисунок 2.3).

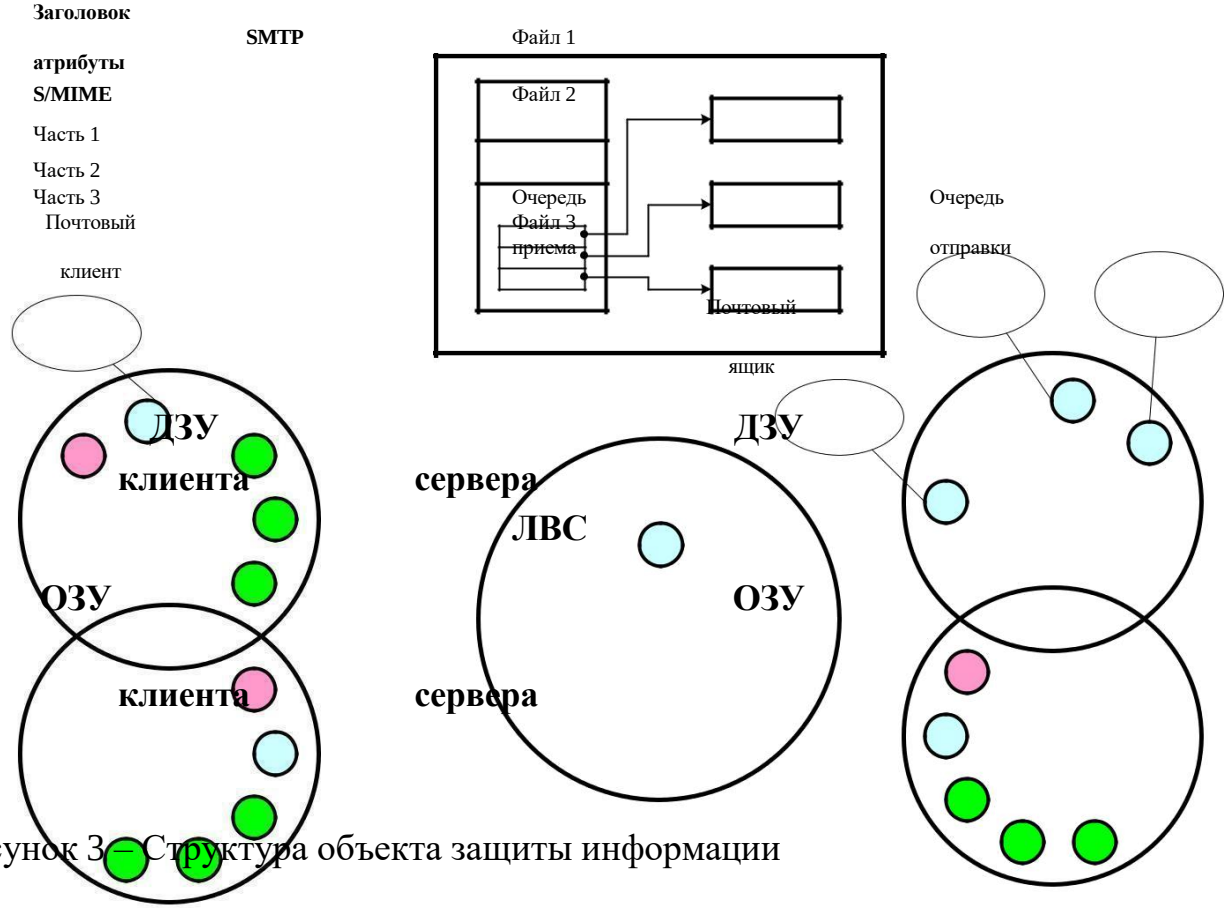


Рисунок 3 – Структура объекта защиты информации

Такое широкое присутствие объекта защиты и его элементов в различных зонах во многом ***определяет сложность задачи комплексной защиты системы электронной почты***. Недостатком такого подхода является то, что для успешной доставки электронного послания необходимым условием является активность средств электронной почты получателя. Если компьютер получателя не работает – электронная почта не будет доставлена. Поэтому разработчики системы электронной почты пошли по другому пути. Они ***разделили задачи доставки и получения почты и сделали их независимыми***. В небольшой организации все перечисленные роли (таблица 1) могут быть закреплены за единственным сервером.

Таблица 1 – Основные функции сервера электронной почты

Роль сервера электронной почты	**Основные функции**
Шлюз электронной почты	– преобразование почтовых сообщений из одного формата в другой, понятный целевой системе электронной почты; – фильтрация электронных сообщений на основе логических правил, применяемых к заголовкам и

	содержимому; – маршрутизация электронных сообщений; – реализация политики информационной безопасности.

Концентратор электронной почты	– обработка входящей почты и доставка ее в почтовые ящики пользователей; – обслуживание почтовых ящиков пользователей; – предоставление доступа к содержимому почтовых ящиков пользователя; – автоматическая обработка почтовых сообщений пользователей.
Сервер пересылки электронной почты	– обработка исходящей электронной почты и доставка электронной почты на один или несколько шлюзов; – преобразование, маскирование адреса отправителя; – тиражирование электронной почты.

В системе электронной почты можно выделить три типа информационных взаимодействий, представленных в таблице 2.2.

Таблица 2 – Типы информационных взаимодействий в системе электронной почты

Тип информационного взаимодействия	**Содержание**	**Сетевой протокол**
Клиент - Сервер	Отправка электронного сообщения одному или нескольким абонентам.	SMTP
Сервер - Сервер	Передача электронных сообщений из очереди исходящих одного сервера в очереди входящих сообщений одного или нескольких серверов, в том числе, в собственную очередь входящих.	SMTP
Сервер - Клиент	Доставка сообщения в один или несколько почтовых ящиков клиентов. Уведомление клиента о наличии новых сообщений в почтовом ящике.	POP3 IMAP

Обратимся теперь к схеме комплексной защиты электронной почты (рисунок 4).

Для того чтобы упростить изучение системы защиты электронной почты, выполним декомпозицию на относительно самостоятельные контуры защиты.

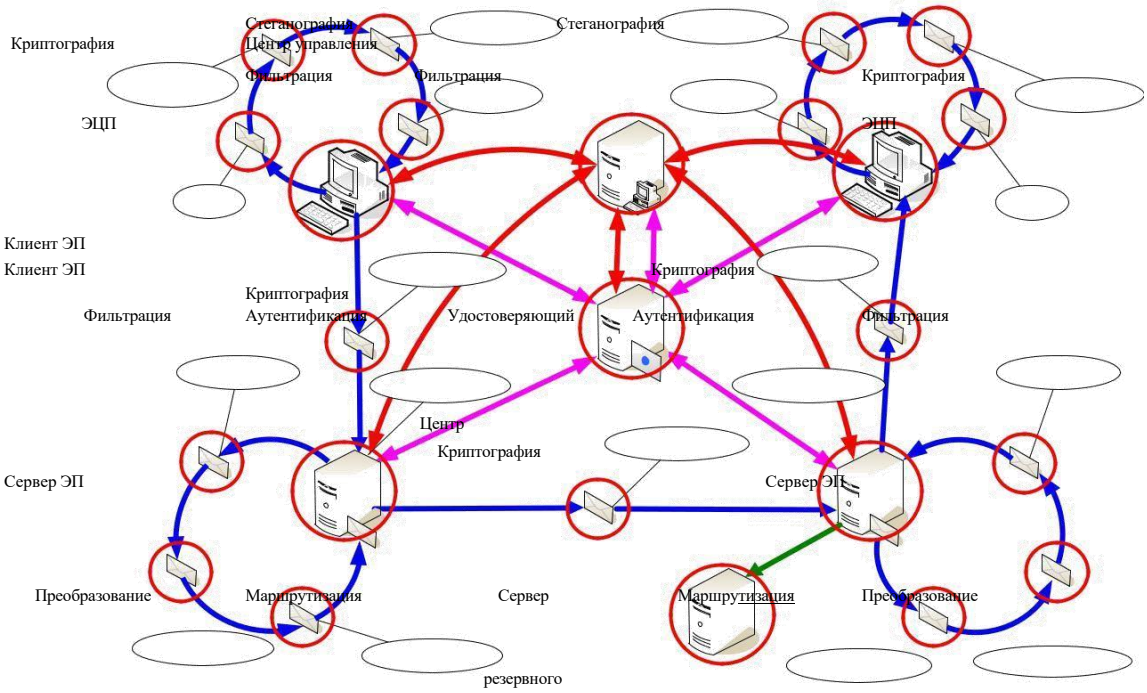
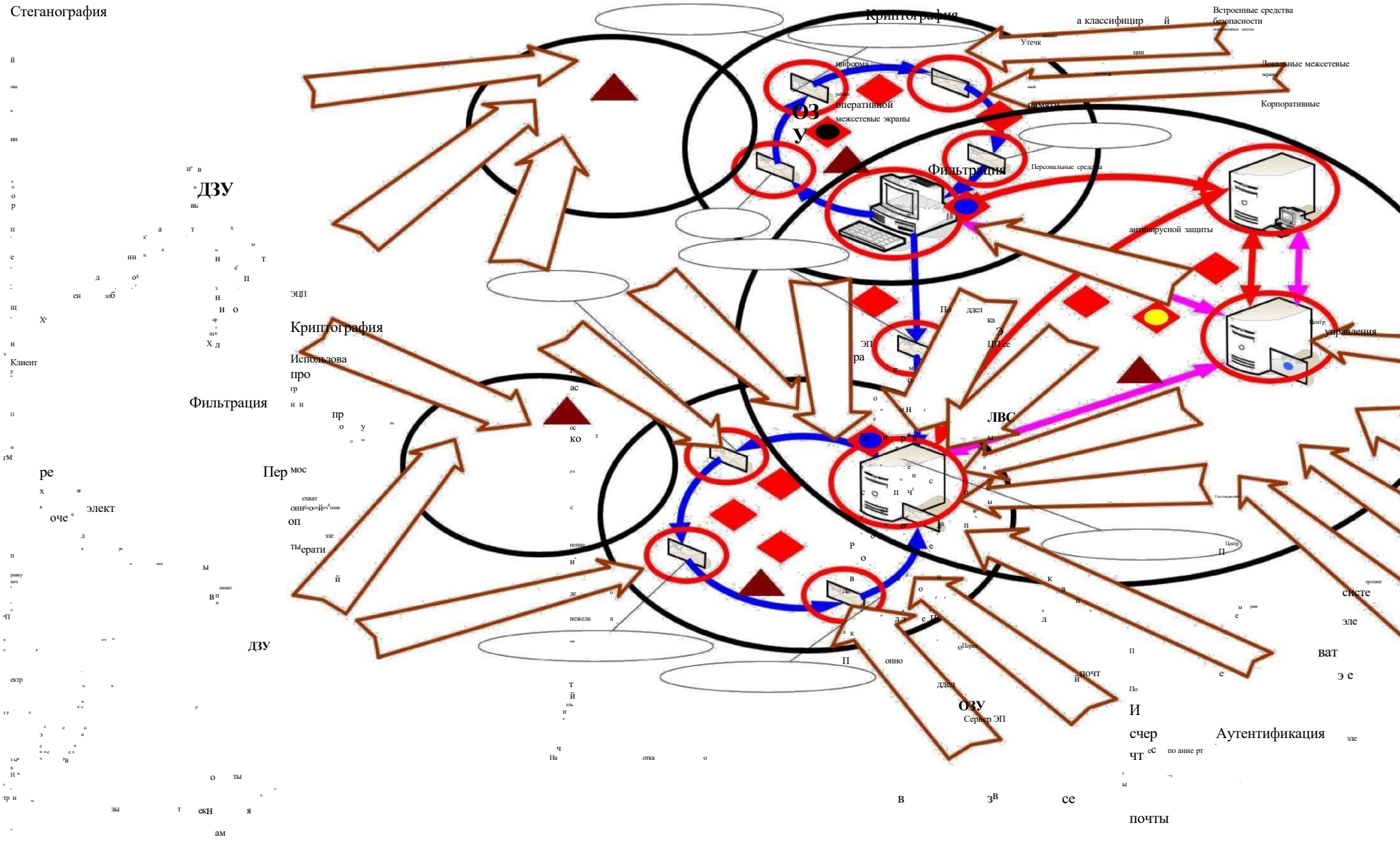


Рисунок 4 – Схема комплексной защиты электронной почты

Реализация контуров защиты электронной почты:
Первый контур защиты соответствует типу взаимодействия «клиент-сервер» (рисунок 5). Дадим характеристику дестабилизирующим воздействиям на зоны и средствам противодействия им.
Типовые нападения на зону ДЗУ клиента электронной почты:
утечка классифицированной информации – наступает вследствие переноса информационных ресурсов из объектов файловой системы в объекты электронной почты, в отсутствии согласованных мер по защите информации;

хищение баз данных электронной почты – хищение носителя с базой данных электронной почты или несанкционированное копирование базы данных электронной почты на носитель злоумышленника позволяет обойти встроенные функции защиты, реализуемые операционной системой и программным обеспечением электронной почты, в отсутствии дополнительных мер и средств защиты информации;
хищение адресных справочников электронной почты –

хищение элементов информационного обеспечения программ электронной почты, в которых хранится информация об известных адресах электронной почты; широкая доступность подобной информации стала причиной одного из негативных явлений сегодняшних дней – рассылки нежелательной корреспонденции (спама).


Стеганография
Криптография
Встроенные средства безопасности
Утечк
Локальные межсетевые экраны
Корпоративные
ОЗУ
оперативной
межсетевые экраны
Фильтрация
Персональные средства
антивирусной защиты
ДЗУ
ЭЦП
Криптография
Использова
про
Клиент
Фильтрация
ЭП
ра
ЛВС
Пер
мос
ДЗУ
управления
ОЗУ
Сервер ЭП
Аутентификация
почты

Преобразование

Об

электронно
й

Рисунок 5 – Первый контур защиты электронной почты

Типовые нападения на зону ОЗУ клиента электронной почты (рисунок 6):

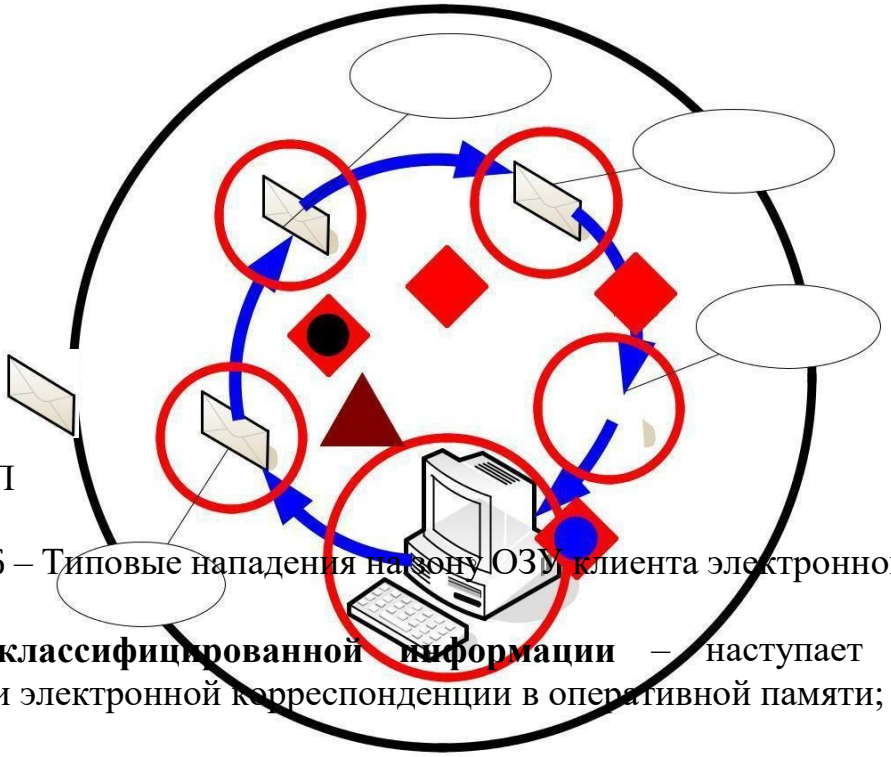


Рисунок 6 – Типовые нападения на зону ОЗУ клиента электронной почты

утечка классифицированной информации – наступает в процессе обработки электронной корреспонденции в оперативной памяти;

перехват электронной почты в оперативной памяти – основная цель нападения - получить доступ к содержимому электронной корреспонденции до того времени, как она будет защищена криптографическими средствами операционной системы или прикладного программного обеспечения.
В зоне ОЗУ реализуются следующие рубежи защиты:
рубеж защиты, образованный средствами операционной системы, выступает как фундамент для дополнительных рубежей: ЭЦП (электронная цифровая подпись), криптография, стеганография, фильтрация.

электронная цифровая подпись служит для подтверждения авторства сообщения электронной почты и контроля его целостности;

криптографическое преобразование позволяет надежно защитить информацию при передаче ее по открытым каналам связи;

стеганография скрывает сам факт передачи информации, маскируя защищенную почтовую связь под малоинтересную переписку обывателей;

5) **средства фильтрации почтовых сообщений**, позволяют блокировать случайную или намеренную отправку классифицированной информации на основе анализа атрибутов и содержания почтового сообщения. Порядок прохождения рубежей может быть произвольным.

Типовые нападения на зону ЛВС, связывающую компьютер клиента электронной почты с сервером электронной почты
(рисунок 7)**:**

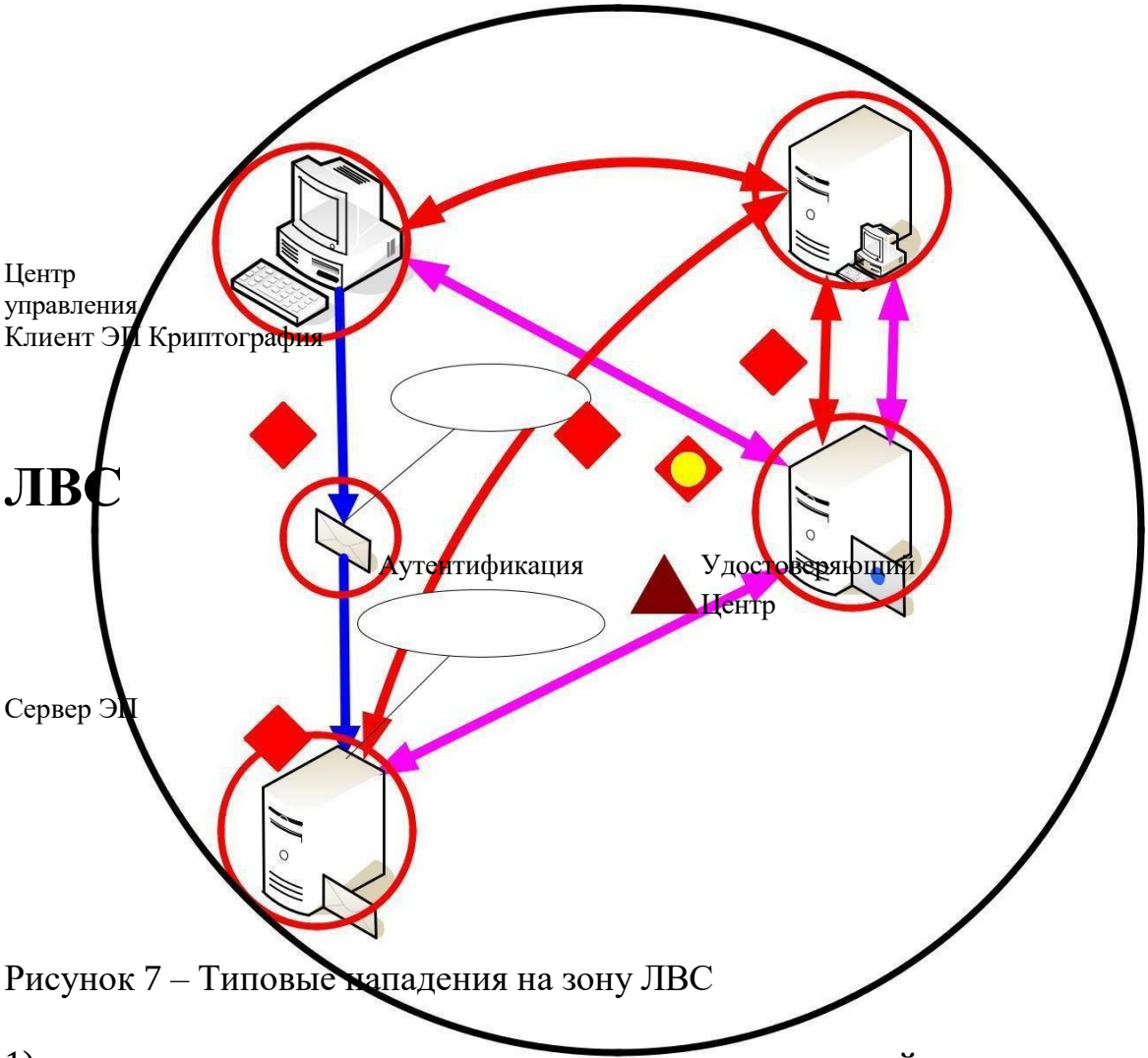


Рисунок 7 – Типовые нападения на зону ЛВС

1) **перехват реквизитов доступа к системе электронной почты** –
цель: путем перехвата сетевых пакетов, относящихся к сеансу работы электронной почты, выделить или восстановить реквизиты доступа к интерфейсу системы электронной почты с тем, чтобы в дальнейшем

злоумышленник мог осуществлять манипуляции с электронной корреспонденцией от лица санкционированного пользователя;

перехват электронной почты – восстановление сообщений электронной почты из перехваченного сетевого трафика в отсутствии надежных средств криптографической защиты информации;
перехват сеанса электронной почты – цель: получить контроль над сеансом почтовой сессии путем подавления средств электронной почты сервера или клиента, с последующим продолжением сеанса средствами злоумышленника.

исчерпание ресурсов сервера электронной почты – отказ в обслуживании – цель: путем создания многочисленных сессий электронной почты или многократной посылки почтовых сообщений в один или более почтовых ящиков исчерпать вычислительные ресурсы сервера и нарушить нормальное функционирование системы электронной почты;
подделка электронной почты – цель: имитация отправки сообщения от имени другого пользователя электронной почты;

подделка ЭЦП сервера или клиента – основанный на явлении коллизий хэш-функций, лежащих в основе постановки электронной цифровой подписи на электронное сообщение, подбор содержания сообщения злоумышленником, в отношении которого проверка ЭЦП дает положительный результат;
компрометация ЭЦП сервера или клиента – раскрытие секретных ключевых параметров ЭЦП сервера или клиента, позволяющее проставлять цифровую подпись на произвольных сообщениях от лица владельца скомпрометированной ЭЦП.
подавление средств защиты электронной почты – использование ошибок реализации или конфигурации средств защиты, позволяющих временно или полностью вывести их из строя. Наиболее подвержены подобным нападениям прицепные, присоединенные средства защиты, или средства защиты, задействуемые по требованиям;
распространение вредоносного программного обеспечения –
использование функциональных средств электронной почты для внедрения программных закладок в ОЗУ или ДЗУ компьютера получателя электронной корреспонденции, как правило, в процессе ее получения или прочтения;

распространениенежелательнойкорреспонденции–
злоупотребление механизмами тиражирования электронной почты для увеличения эффекта информационного воздействия, как правило, в целях рекламы;

использование уязвимостей программного обеспечения электронной почты – использование ошибок прикладного программного

обеспечения электронной почты для получения контроля над компьютером, где оно выполняется.

Основные рубежи защиты образуются средствами сетевых операционных систем на каждом из сетевых узлов. В результате согласованного взаимодействия криптографических средств сетевых узлов образуется ***рубеж защиты на этапе передачи информации в сети***.

Криптографическая защита электронной почты может реализовываться:

взаимодействием криптографических средств программного обеспечения электронной почты;

взаимодействием криптографических средств операционных систем клиента и сервера электронной почты;

аппаратно-программными средствами межсетевых экранов и телекоммуникационного оборудования.

целях раннего обнаружения и предупреждения нападений на систему электронной почты в зоне ЛВС располагаются сенсоры сетевой системы обнаружения вторжений. Сенсоры могут располагаться

непосредственно в сети, осуществляя прослушивания всего сетевого трафика на предмет признаков угроз системам электронной почты, или же внедряться сетевые компоненты операционных систем узлов электронной почты.

Контроль над распространением электронной почты возлагается на средства межсетевых экранов и телекоммуникационного оборудования.

На зону ОЗУ сервера осуществляются следующие типовые нападения:

перехват электронной почты в оперативной памяти

навязывание электронной почты в оперативной памяти обход фильтров электронной почты

навязывание маршрутизации электронной почты

В ОЗУ сервера реализуются следующие рубежи защиты (рисунок 8):

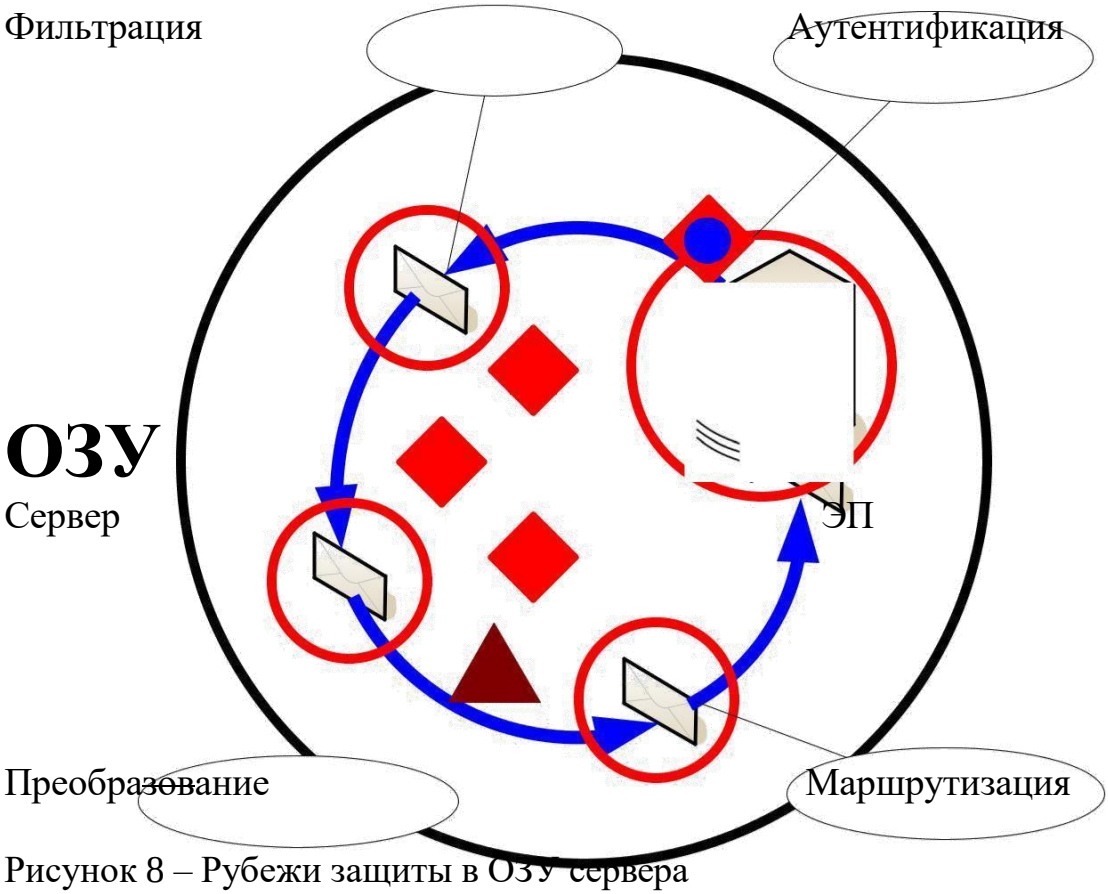


Рисунок 8 – Рубежи защиты в ОЗУ сервера

Основной рубеж образуют встроенные средства системного и прикладного программного обеспечения операционной системы сервера и электронной почты. Важнейшие функции: аутентификация и криптографическая защита канала передачи данных.

На основе вышеописанного рубежа реализуются ***дополнительные рубежи:*** фильтрация, преобразование, маршрутизация.

Рубеж фильтрации предназначен для борьбы с утечкой классифицированной информации, с распространением вредоносного программного обеспечения и нежелательной корреспонденции, он также участвует в реализации политики управления информационными потоками.

Рубеж преобразования на основе системы правил выполняет модификацию заголовков и содержимого электронного сообщения. Задача данного рубежа скрыть внутреннюю структуру организации, замаскировать каналы обмена информацией, реализовать централизованную криптографическую защиту сообщений электронной почты.

Рубеж маршрутизации выполняет основную работу по управлению информационными потоками. Именно здесь принимаются решения об отправке электронной почты по защищенному или открытому каналу связи.

Дополнительной задачей рубежа является реализация отказоустойчивости за счет использования избыточных каналов связи.

На зону ДЗУ сервера электронной почты осуществляются следующие нападения:

перехват электронной почты в очереди на отправку;

навязывание электронной почты в очередь на отправку. Переходим к описанию следующего контура защиты. Данный контур описывает защиту взаимодействия «сервер-сервер» (рисунок 9).

Типовыми нападениями на зону ЛВС, связывающую два сервера электронной почты, являются:

изменение топологии, архитектуры системы электронной почты – цель: воздействуя на средства управления системой электронной почты, изменить топологию информационных связей наиболее выгодным для намерений злоумышленника образом;

сокрытие фактов нападения на систему электронной почты – цель: воздействуя на средства управления (средства регистрации событий) скрыть источник нападения или сам факт нападения на систему электронной почты;

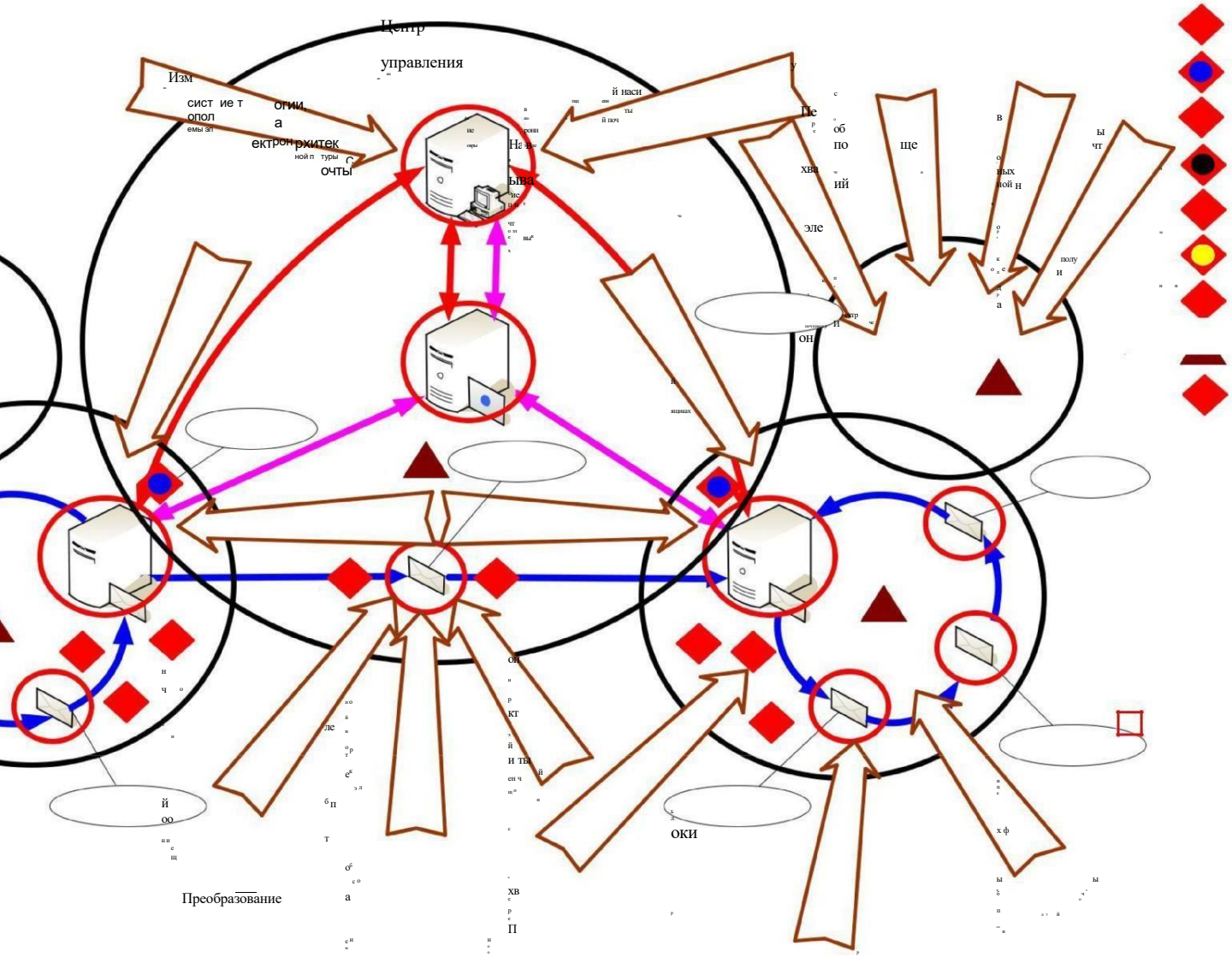

Центр
управления
Преобразование
Маршрутизация
онание

Рисунок 9 – Контур защиты взаимодействия «сервер – сервер»

имитация ошибок сеанса обмена электронными сообщениями – цель: воздействуя на сервер-отправитель, сымитировать ситуацию «неполучения» электронной корреспонденции;

дезавуирование абонентов электронной почты – цель: используя служебные функции сервера-получателя, выяснить состав обслуживаемых сервером абонентов, получить список адресов электронной почты сервера- получателя;

ложный сервер-отправитель – цель: имитировать сеанс отправки сообщения с санкционированного сервера-отправителя, при активном подавлении последнего;

ложный сервер-получатель – цель: имитировать сеанс приема сообщения санкционированным сервером-получателем, при активном подавлении последнего;

подмена сообщений электронной почты – цель: используя контролируемые телекоммуникационные средства, блокировать отправленное сообщение, и, используя его реквизиты почтовой сессии, навязать сообщение злоумышленника;

перехват сообщений электронной почты – цель: путем прослушивания сетевого трафика захватить сетевые пакеты сеанса электронной почты и восстановить почтовые сообщения, переданные в ходе него;

блокирование сообщения электронной почты – цель: с помощью служебных сообщений электронной почты или подконтрольного злоумышленнику телекоммуникационного оборудования, нарушить штатную работу электронной почты, сделать невозможным электронный документооборот.

В зоне ЛВС реализованы рубежи защиты, показанные на рисунке10.

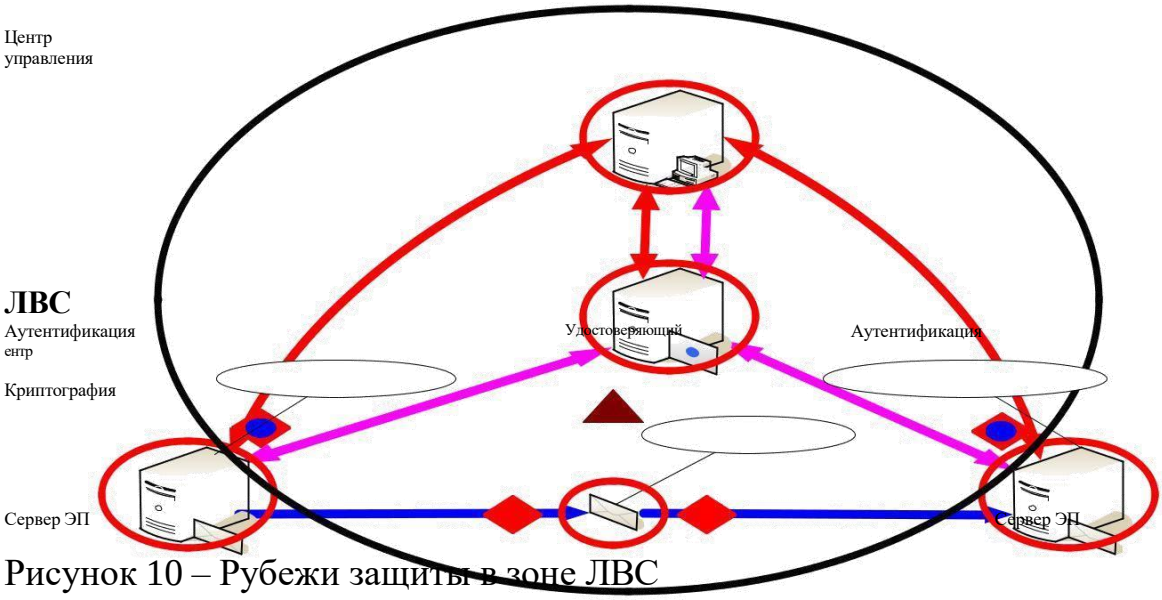


Рисунок 10 – Рубежи защиты в зоне ЛВС

В результате взаимодействия криптографических средств защиты сетевых операционных систем, межсетевых экранов и телекоммуникационного оборудования образуется ***рубеж криптографической защиты.***

Против зоны ОЗУ сервера-получателя применяются следующие типовые нападения:

использование служебных функций электронной почты – цель: сбор информации о системе электронной почты, организация атак типа «отказ в обслуживании», использование изъянов программного обеспечения его конфигураций;

похищение услуг, сервисов электронной почты – цель: используя изъяны конфигурации программного обеспечения и средств защиты сервера-получателя, вынудить выполнить его дополнительные функции, например, пересылку или тиражирование почты, автообработку почтового сообщения, ввод информации в базу данных и т. п.

3) **обход фильтров электронной почты** – цель: с помощью криптографических или специальных преобразований затруднить или сделать полностью неэффективной работу фильтров сервера получателей,

реализующих политику управления информационными потоками или политику информационной безопасности.

В зоне ОЗУ сервера-получателя образуются рубежи защиты, показанные на рисунке 11:

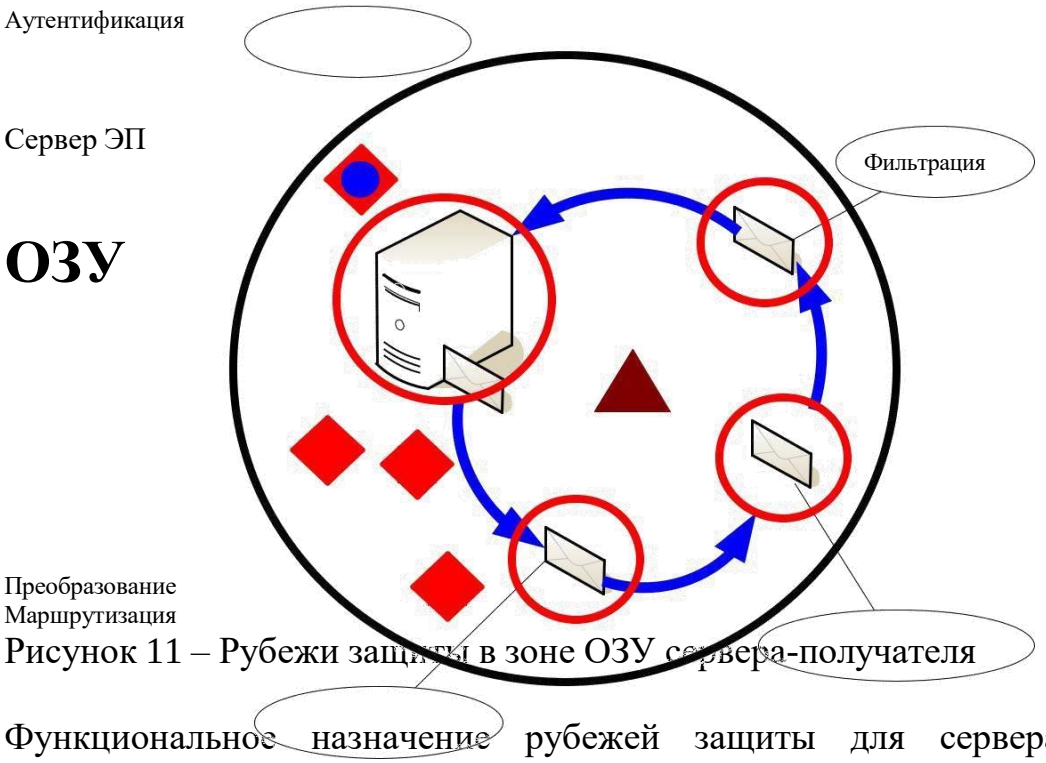


Рисунок 11 – Рубежи защиты в зоне ОЗУ сервера-получателя

Функциональное назначение рубежей защиты для сервера-получателя зеркально-симметрично аналогичным рубежам сервера-отправителя.

Основной рубеж образуют встроенные средства системного и прикладного программного обеспечения операционной системы сервера и электронной почты. ***Важнейшие функции: аутентификация и криптографическая защита канала передачи данных***.

На основе вышеописанного рубежа реализуются ***дополнительные рубежи: фильтрация, преобразование, маршрутизация.***

Рубеж фильтрации предназначен для борьбы с навязыванием ложной информации, с распространением вредоносного программного обеспечения и нежелательной корреспонденции, он также участвует в реализации политики управления информационными потоками.

Рубеж преобразования на основе системы правил выполняет модификацию заголовков и содержимого электронного сообщения. Задача данного рубежа - скрыть внутреннюю структуру организации, замаскировать каналы обмена информацией, реализовать централизованную криптографическую защиту сообщений электронной почты.

Рубеж маршрутизации выполняет основную работу по управлению информационными потоками. Именно здесь принимаются решения о доставке электронной почты на тот или иной концентратор электронной

почты. Дополнительной задачей рубежа является реализация отказоустойчивости за счет использования избыточных каналов связи.

Против зоны ДЗУ сервера-получателя реализуются следующие нападения:

навязывание электронной почты в почтовых ящиках пользователей – цель: используя прямой доступ к базе данных концентратора электронной почты, навязать в почтовый ящик одного или более пользователей сервера сообщения электронной почты. Наибольшую угрозу этот вид нападения представляет для крупных серверов электронной почты, например, серверов, обслуживающих системы mail.ru, yandex.ru и

т.п.;

перехват электронной почты в почтовых ящиках пользователей
– цель: используя прямой доступ к базе данных концентратора электронной почты или к файлам базы данных, восстановить сообщения отдельных пользователей с последующей передачей на компьютер злоумышленника;

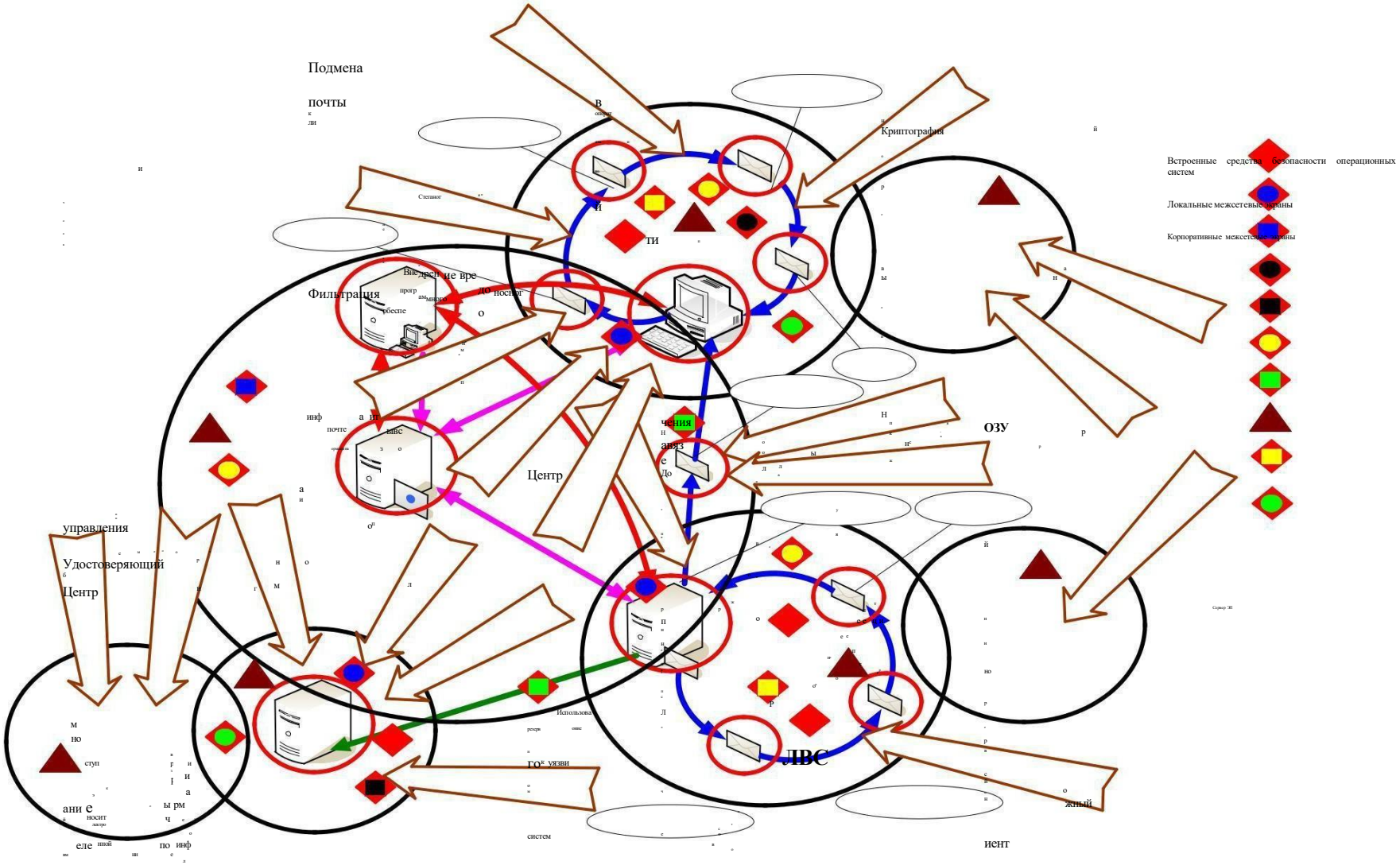
перехват электронной почты в очереди полученных сообщений
– цель: используя прямой доступ к файлам и папкам концентратора электронной почты или механизмы межпроцессного взаимодействия, получить доступ к сообщениям электронной почты;

навязывание электронной почты в очереди полученных сообщений – цель: используя прямой доступ к файлам и папкам концентратора электронной почты или механизмы межпроцессного взаимодействия, навязать сообщения электронной почты, которые в дальнейшем будут подвергнуты штатной обработке средствами программного обеспечения электронной почты.

Защита электронной корреспонденции в зоне ДЗУ осуществляется криптографическими средствами операционных систем и программного обеспечения электронной почты, а также средствами контроля целостности.

Последний контур защиты описывает взаимодействие «сервер-клиент». В дополнение к рассмотренным выше нападениям на зону ОЗУ сервера-получателя в контексте данного контура защиты воздействует доступ к

интерфейсу почтового ящика в оперативной памяти – в стандартных серверах электронной почты функции работы с почтовым ящиком сгруппированы в одну библиотеку, с помощью специальной собранной программы можно посредством данной библиотеки обратиться к почтовому ящику и выполнить манипуляции с ним (рисунок 12).


Подмена
почты
Криптография
Встроенные средства безопасности операционных систем
Локальные межсетевые экраны
Корпоративные межсетевые экраны
Фильтрация
Центр
ОЗУ
ЛВС

ДЗУ

ани

ыв

Персональные средства антивирусной защиты

Ы да

Системы обнаружения атак и проактивной защиты

Сетевые средства криптографической защиты

Вредоносное

программное д

обеспечение

Переехат

Средства контентной фильтрации

к почтовому

ящику

Локальные средства криптографической защиты

АутентификацияФильтрация

ОЗУ

ДЗУ

копирова

ДЗУ

Сервер
резервного

Рисунок 12 – Контур защиты взаимодействия «сервер-клиент»

Рубежи защиты сервера-получателя представлены на рисунке 13.

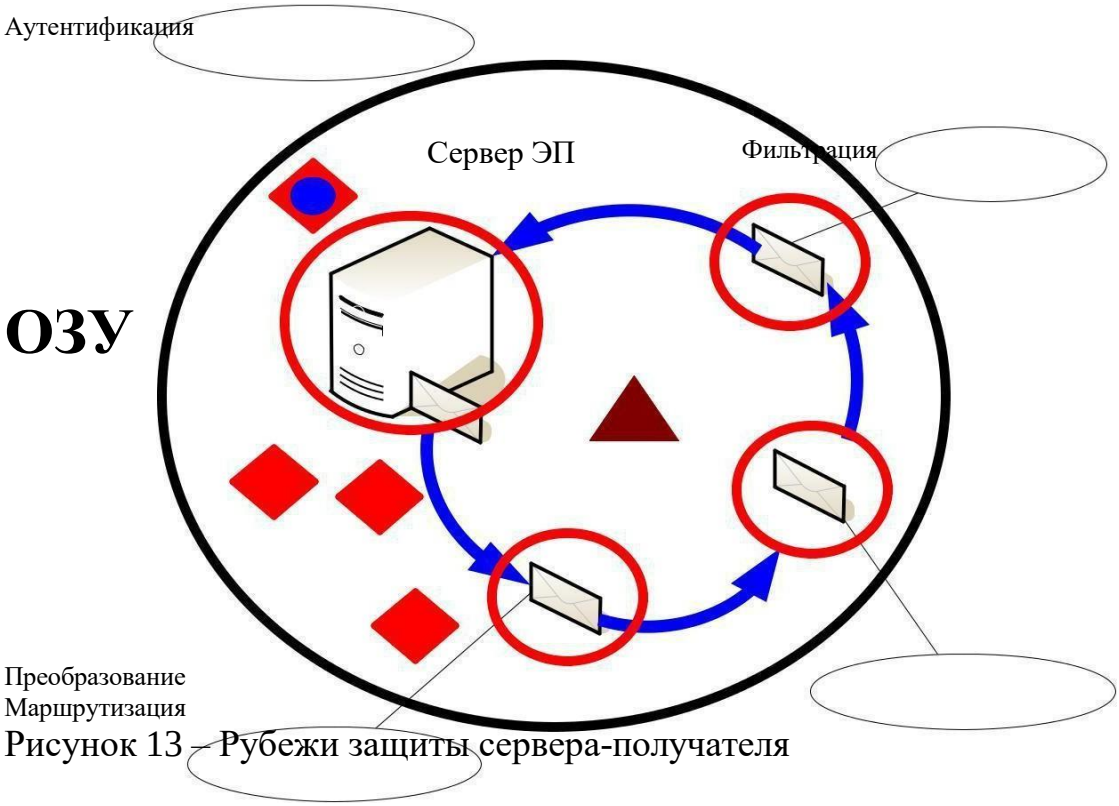


Рисунок 13 – Рубежи защиты сервера-получателя

На зону ДЗУ сервера получателя дополнительно воздействует угроза прямого доступа к носителю с почтовым ящиком пользователя.

К зоне ОЗУ клиента-получателя применяются следующие типовые нападения (рисунок 2.14):

внедрение вредоносного программного обеспечения – цель:
используя средства автоматической обработки почтовых сообщений программным обеспечением клиента электронной почты, внедрить в программную среду клиента программные закладки (вредоносное программное обеспечение);

подмена почтового сообщения в оперативной памяти – цель:
заменить содержание почтового сообщения, полученного с сервера, содержимым сообщения злоумышленника путем модификации участка программного кода, ответственного за этот этап прохождения электронной почты;

навязывание почтового сообщения в оперативной памяти –
цель: воздействуя на структуры динамической памяти, навязать сообщение электронной почты, имитируя его прием в текущей почтовой сессии.

Рубежи защиты клиента-получателя представлены на рисунке 14.

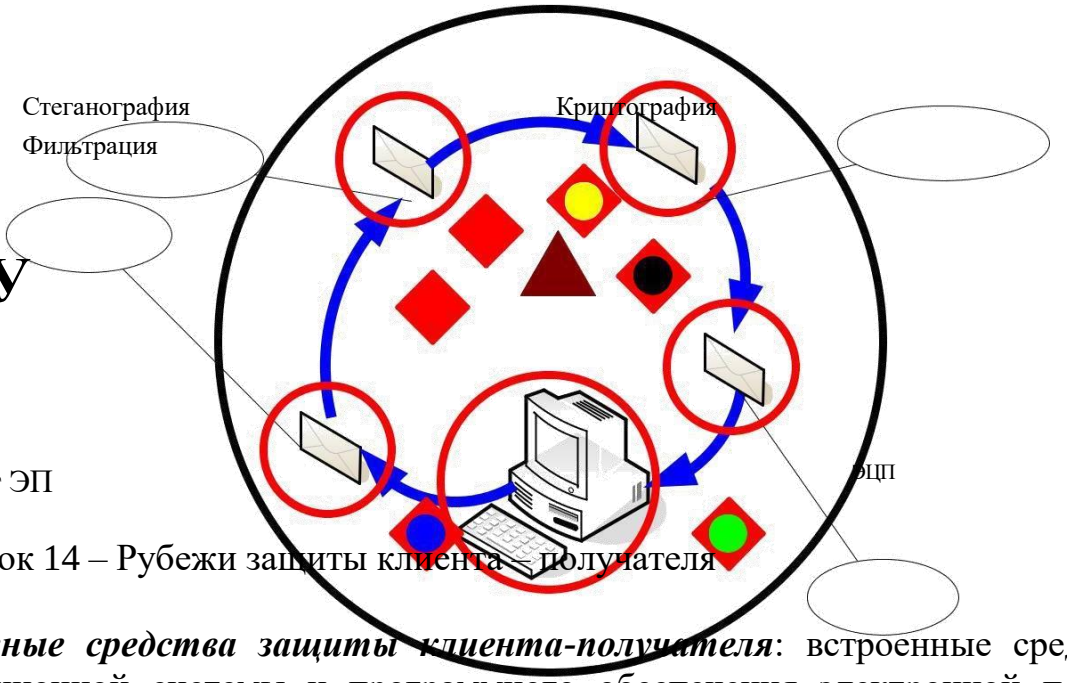


Рисунок 14 – Рубежи защиты клиента – получателя

Основные средства защиты клиента-получателя: встроенные средства операционной системы и программного обеспечения электронной почты, антивирусные программные средства, средства контентной фильтрации.

Против зоны ДЗУ сервера резервного копирования существуют следующие типовые нападения:

доступ к электронной почте на резервном носителе информации – цель: хищение или несанкционированное копирование носителя информации с резервной копией сообщений электронной почты;

навязывание электронной почты на резервный носитель информации – цель: путем замены или модификации носителя с резервной копией сообщений электронной почты и последующим инспирированием сбойной ситуации, добиться восстановления навязанной информации на сервере электронной почты.

Основные средства защиты информации: средства контроля целостности и криптографической защиты носителей с резервной копией.

Зоне ОЗУ сервера резервного копирования угрожают следующие типовые нападения:

использование уязвимостей системы резервного копирования – цель: воздействуя на ошибки программного обеспечения и изъяны конфигурации получить контроль над сервером резервного копирования;
резервное копирование с ложного сервера – цель: подавляя средства резервного копирования санкционированного сервера, выполнить резервное копирование ложной информации на сервер резервного копирования с последующей инспирацией сбойной ситуации и восстановления с навязанной резервной копии;
восстановление на ложный сервер – цель: хищение сообщений электронной почты путем имитации сбоя на санкционированном сервере электронной почты и последующего перехвата сеанса восстановления информации из резервной копии, с подавлением санкционированного сервера электронной почты;
перехват электронных сообщений в оперативной памяти – цель: с помощью программной закладки получить доступ к электронным сообщениям в оперативной памяти сервера резервного копирования на этапе подготовки к сохранению на резервном носителе информации.

Для отражения этих нападений в зоне ОЗУ сервера резервного копирования создаются рубежи защиты, представленные на рисунке 15.

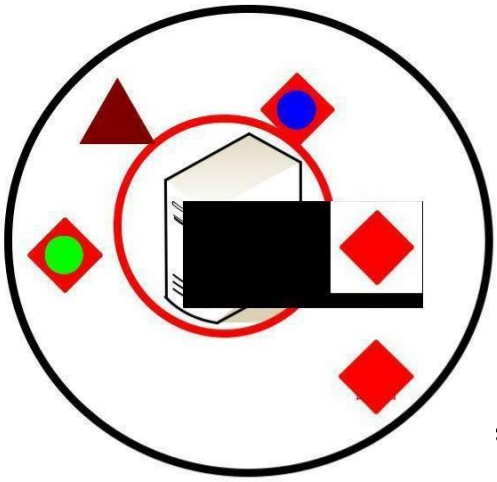


Рисунок 15 – Рубежи з рвного копирования

В реализации рубежа защиты сервера резервного копирования участвуют встроенные средства защиты операционной системы и программного обеспечения системы резервного копирования.

Для зоны ЛВС, связывающей клиента, сервер электронной почты и сервер резервного копирования, характерны следующие типовые нападения:

перехват электронной почты – цель: восстановить сообщения электронной почты из перехваченных сетевых пакетов сеансов взаимодействия клиента с сервером электронной почты;

перехват реквизитов доступа к почтовому ящику – цель: извлечение или восстановление реквизитов доступа санкционированного пользователя к содержимому почтового ящика;

распространение вредоносного программного обеспечения – цель: используя средства автоматической обработки входящей электронной почты, внедрить программные закладки, вредоносное программное обеспечение в программную среду компьютера клиента системы электронной почты;

распространение нежелательной корреспонденции – цель: использование ставшего известным злоумышленнику адреса электронной почты для доставки адресного информационного воздействия пользователю электронной почты;

ложный сервер – цель: активно подавляя санкционированный сервер электронной почты, похитить реквизиты доступа у клиента электронной почты или же навязать ему электронную почту злоумышленника;

ложный клиент – цель: активно подавляя санкционированного клиента, воспользоваться его почтовой сессией для доступа к информации почтового ящика

Основные рубежи защиты зоны ЛВС показаны на рисунке 16.

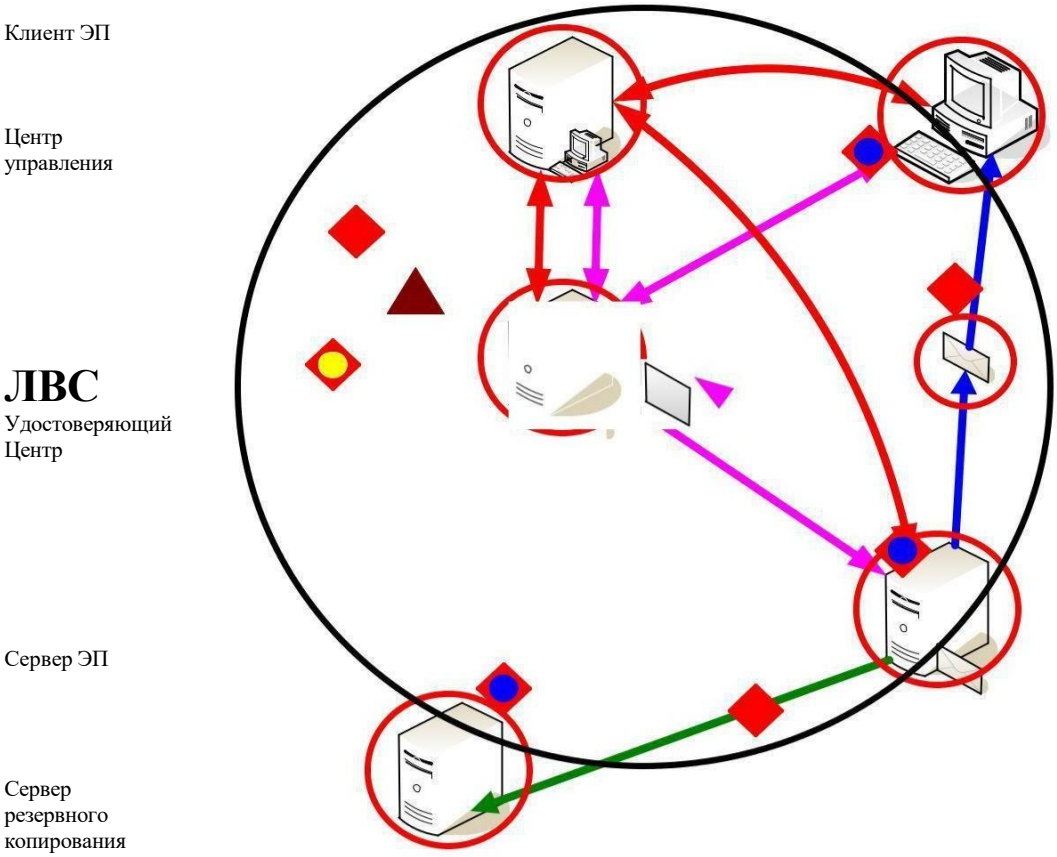


Рисунок 16 – Основные рубежи защиты зоны ЛВС

Взаимодействие встроенных средств защиты операционных систем и программного обеспечения электронной почты и резервного копирования образуют криптографические рубежи защиты информации в сети. Стойкость данных рубежей может быть усилена привлечением аппаратно-программных средств межсетевых экранов и телекоммуникационного оборудования.

Управление криптографическими средствами защиты информации осуществляется на основе инфраструктуры открытого ключа с помощью общего удостоверяющего центра.

Применение криптографии с открытыми ключами для обеспечения информационной безопасности:

Криптографические алгоритмы используются для шифрования открытого текста (plaintext) с использованием ключа шифрования (encryption key), в результате чего получаются зашифрованные данные (ciphertext).

Зашифрованный по надежному криптографическому алгоритму текст практически невозможно расшифровать без дополнительных данных, которые называются ключом расшифрования (decryption key).

В криптографии с симметричными ключами (symmetric key) для шифрования и расшифрования ***используется один и тот же секретный ключ*** (secret key), то есть ключ шифрования совпадает с ключом расшифрования. Стороны могут передавать друг другу данные, зашифрованные секретным ключом, только после того, как они обменяются этим общим ключом.

При шифровании с открытым ключом у каждого пользователя должно быть два ключа – открытый (public) и личный (private) – секретный ключ. Если открытый ключ сделать общедоступным, пользователи смогут отправлять вам зашифрованные с его помощью данные, которые только Вы будете способны расшифровать с помощью своего личного секретного ключа. С помощью личного ключа Вы также можете преобразовать отправляемые данные таким образом, что пользователи смогут удостовериться в том, что

эти данные были отправлены именно вами, а не кем-то другим. Эта возможность служит основой цифровых подписей.

Различие ключей – открытого и личного – в криптографии с открытыми ключами ***позволило создать следующие технологии: электронные цифровые подписи, распределенная проверка подлинности, согласование общего секретного ключа сессии, шифрование больших объемов данных без предварительного обмена общим секретным ключом***.

Создание и проверка электронных цифровых подписей (digital signature) – это, вероятно, самый интересный аспект криптографии с открытыми ключами. ***Основой электронной цифровой подписи является математическое преобразование подписываемых (signed) данных с использованием личного секретного ключа*** и выполнением следующих условий:

создать электронную цифровую подпись можно только с использованием личного секретного ключа;

проверить действительность электронной цифровой подписи может любой, имеющий доступ к соответствующему открытому ключу;

любое изменение подписанных данных (даже изменение всего одного бита в большом файле) делает электронную цифровую подпись недействительной.

Криптография с открытыми ключами обеспечивает надежные службы распределенной аутентификации.

Технология шифрования с открытым ключом позволяет шифровать большие объемы данных в том случае, если у обменивающихся информацией сторон нет общего ключа.

В настоящее время наиболее часто используются сертификаты на основе стандарта Международного союза телекоммуникаций ITU-T X.509

версии 3 и рекомендаций IETF (Internet Engineering Task Force) RFC 2459.

Это базовая технология, используемая в инфраструктуре открытых ключей операционной системы Windows 2000. Это не единственный вид сертификатов. Например, система защиты сообщений электронной почты

PGP (Pretty Good Privacy) использует свою специфическую форму сертификатов.

Центр сертификации (ЦС) – это служба, которая выдает сертификаты. Центр сертификации является гарантом связи между открытым ключом субъекта и содержащейся в сертификате информацией по идентификации этого субъекта. Различные ЦС устанавливают и гарантируют эту связь различными способами, поэтому прежде чем доверять сертификатам того или иного ЦС, следует ознакомиться с его политикой и регламентом.

Включенные в операционную систему Windows 2000 службы сертификации предоставляют предприятию средства для организации центров сертификации. ***Службы сертификации содержат применяемый по умолчанию модуль политики, который можно использовать для выдачи сертификатов пользователям, компьютерам и службам***. При этом выполняется идентификация объекта, отправившего запрос сертификат, и проверка допустимости запрошенного сертификата соответствии с политикой безопасности домена. Разработчики могут изменить этот модуль таким образом, чтобы он соответствовал другой политике, а также расширить поддержку ЦС для различных сценариев Интранета и Интернета.

Инфраструктура открытых ключей предполагает иерархическую модель построения центров сертификации. Такая модель обеспечивает масштабируемость, удобство администрирования и согласованность с растущим числом коммерческих продуктов и ЦС различных поставщиков.

Простейшая форма иерархии ЦС состоит из одного ЦС, а в общем случае – из множества ЦС с явно определенными отношениями родительский-дочерний. Допускается существование не связанных между собой иерархий.

Другими словами, ***центры сертификации не обязательно должны иметь общий родительский (корневой) ЦС на самом верхнем уровне.***

В этой модели дочерние ЦС сертифицируются родительским ЦС. ЦС, находящийся на самом верхнем уровне иерархии, обычно называется корневым (root) ЦС. Подчиненные ЦС являются промежуточными (intermediate) или выдающими (issuing) ЦС. ***Выдающим ЦС называется тот центр сертификации, который выдает сертификаты конечным пользователям.***

Промежуточным ЦС здесь называется тот ЦС, который не является корневым и выдает сертификаты только другим ЦС, а не конечным пользователям.

Фундаментальное преимущество этой модели состоит в том, что проверка сертификатов требует доверия только относительно малому числу корневых ЦС. В то же время эта модель позволяет иметь различное число ЦС, выдающих сертификаты.

Поддержка нескольких выдающих ЦС применяется по ряду причин практического свойства. К ним относятся следующие:

использование. Сертификаты могут выдаваться для различных целей (например, для защиты электронной почты, сетевой аутентификации и так далее). Политика выдачи сертификатов для этих целей может быть различной, а существование нескольких ЦС позволяет реализовать различные политики;

структура подразделений организации. Политики выдачи сертификатов могут различаться в зависимости от роли субъекта в организации. Для разделения этих политик и управления ими можно создать несколько выдающих ЦС;

территориальное деление. Организации могут иметь территориально отдаленные подразделения. Из-за условий сетевой связи между этими подразделениями может потребоваться несколько выдающих ЦС.

Использование СКЗИ КриптоПро CSP позволяет решить сразу несколько задач:

корпоративные пользователи получают возможность использовать стандартные и повсеместно используемые приложения корпорации Microsoft с надежной российской криптографией (256 бит);

системные интеграторы получают возможность создавать новые, надежно защищенные приложения, используя проверенный временем инструментарий разработки корпорации Microsoft.

стандартным приложениям, которые теперь могут использовать российские алгоритмы электронной цифровой подписи и шифрования, относятся:

центр Сертификации сертификатов открытых ключей X.509 — Microsoft Certification Authority;

электронная почта – Microsoft Outlook, входящая в состав Microsoft Office 2000;
электронная почта – Microsoft Outlook Express, входящая в состав Internet Explorer версии 5.0 и выше;
средства формирования и проверки электронной цифровой подписи программных компонент, распространяемые по сети – Microsoft Authenticode;
защита соединений в Интернете с использованием протокола TLS/SSL.

Борьба со спамом:

Чтобы спам попал в ваш ящик, его необходимо вам доставить.
Первые виды спама были просто прямыми рассылками. Такой спам блокируется достаточно просто, и спамеры начали использовать ***открытые почтовые релеи, то есть обычные почтовые сервера, позволяющие произвольному пользователю воспользоваться сервисом отправки письма***

на другой сервер. Заметим, что иных релеев в ту пору просто не было, а само понятие «открытые релеи» возникло лишь после того, как появился спам и их вообще начали закрывать.

Такие открытые релеи достаточно легко детектировать, их стали активно искать и блокировать. После этого у прямых рассылок наступил ренессанс – спам стал рассылаться с «диалапов» и для его блокирования системным администраторам пришлось разузнавать и блокировать IP модемных пулов основных провайдеров.

Затем ***появились*** как заметное явление более ***изощренные способы использования чужих, неаккуратно сконфигурированных серверов***. Socks-прокси серверы предназначены для сведения всего интернет-трафика небольших компаний к одной единственной машине, имеющей доступ в Интернет. Для работы они обычно используют порт 1080. Если машина допускает неавторизованное соединение с произвольного IP-адреса (типичная ситуация в эру до спама), ее могут использовать спамеры и для направления своего SMTP-трафика. Логи использования socks-серверов обычно не ведутся, поэтому отслеживание истинных источников рассылки даже самими администраторами socks-серверов чаще всего невозможно.

Почти сразу же обнаружилось, что и стандартные открытые HTTP-прокси (типичные порты 3128, 8080 и т.д.), поддерживающие метод CONNECT, легко использовать для того же самого, достаточно в команде CONNECT указать не только имя сервера, но и задать 25-й почтовый порт. Даже «народный» вебсервер Apache, собранный с модулем mod_proxy и неправильно настроенный, нередко используют как средство рассылки почтового спама.

Софт для прямых рассылок (например Advanced Mail Sender), в котором спамер в обход сервера провайдера обращается к целевому MTA прямиком с домашнего модема, сменился продвинутыми сложными системами, вершиной которых являются троянские кони широкого спектра действия. Среди их возможностей есть даже апгрейд самих себя, автоматическое распространение, переезд на другие взломанные машины и т.д.

Есть много способов скрыть троянскую программу: использовать нестандартные порты, управление, протоколы и т.д. и т.п.

Для более или менее серьезной борьбы со спамом интереснее знать, кто этот троян распространяет и как он это делает. Для подобных выяснений и полезны администраторы сетей, в которых есть зараженные машины. Например, если троян ходит куда-то зачем-то по HTTP, то, во-первых, надо засечь это обращение и его содержание, а также ответ той стороны, а во-вторых, отследить входящие соединения с ним, их источники и суть.

У спамеров существует разделение труда – категория «взломщиков» выделилась в отдельную профессию, а товаром и предметом купли-продажи служат списки IP-адресов. Покупателями являются «рассылочники». Сетевое сообщество не смогло до сих пор внедрить простейшие антиспамерские

приемы, которые само же установило в качестве стандарта. Например, разделение портов SMTP-сервера на порт для MTA (25: прием почты от

чужого сервера для сохранения своему пользователю; «общение между серверами») и MSA (587: прием письма от своего пользователя для отправки на чужой сервер; «общение между пользователем и сервером»). Эта идея, также как и SMTP-авторизация, появилась именно как реакция на появление спама.

Данные, которые используются для анализа – это все признаки пришедшего письма. Их можно разделить на четыре пространства, вычисление решений в которых можно производить независимо:

IP-адрес сервера-отправителя;

оформление и стиль писем, заголовки, форматирование, характерные обороты;

статистика слов в письмах;

контрольные суммы («сигнатуры») текстов писем.

Естественно, что пространство признаков по каждому набору данных ограничивают только «интересными» признаками. Конкретный антиспамовый модуль может использовать все пространства признаков или только 1-2 из них. Недостатки и преимущества каждого из пространств признаков обсудим ниже. Обратим внимание на необходимое присутствие еще двух составляющих «задачи машинного обучения», классическим примером каковой является детектор спама, а именно: обучающей выборки и обратной связи.

В отличие от пространств слов или элементов оформления, при опознании спама по IP-адресу решение принимается по одному-единственному признаку. Взвешивания по адресу обычно не производится, следовательно, настройка взвешивающего механизма на обучающей выборке не нужна. Однако без обратной связи (в случае с IP – без постоянно пополняемого списка черных дыр) удовлетворительно работающий механизм нельзя построить ни по одному из вышеперечисленных пространств.

Чтобы любое машинное обучение работало, ему необходимо сообщать об ошибках. ***Ошибки бывают двух видов***. Ошибка первого рода: пропуск спама, то есть пропуск спамового письма. Иными словами – недостаточная полнота метода. Ошибка второго рода – ложные срабатывания, когда не-спам ошибочно относят к спаму. Иными словами – точность метода.

Приоритет при настройке алгоритма отдается минимизации числа ложных срабатываний. Обычное требование для спам-детектора – уложиться в несколько промилле. Считается, что лучше дать пользователю прочитать несколько спамовых писем, чем скрыть от него настоящее письмо. Процент детектированного спама есть мера полноты, процент ложных срабатываний – мера неточности. Несложно предложить интегральную

оценку качества, назовем ее качеством фильтрации. Очевидно, что при точности, близкой к 100%, качество будет примерно равно полноте. Именно полноту фильтрации часто и называют, когда озвучивают те или иные цифры, подразумевая, что точность практически абсолютна.
Острота восприятия ошибки второго рода зависит от характера поступающих в почтовый ящик писем и индивидуальных предпочтений пользователя: люди, обсуждающие в почте многомиллионные сделки, реагируют на ошибки второго рода гораздо более болезненно, чем сервис поддержки пользователей.
Очень важная, часто недопонимаемая проблема состоит в том, что спам и не-спам пересекаются в очень большой степени.
Рассылки, от которых трудно отписаться, но на которые Вы (кажется?) подписывались. Подписки, возникающие при регистрации, без Вашего ведома. Многочисленные квитанции антиспамерских и антивирусных программ. Автоответчики. Рассылки, совершаемые спамерами при помощи веб-форм из публичных, совершенно неспамерских веб-сервисов, слабо защищенных от вторжения. Вся такая корреспонденция может быть смело отнесена к «полуспаму». Объем этой зоны очень и очень значительный.
Даже с учетом статистических смещений, характерных для публичной веб-почты, можно попытаться предсказать максимальный теоретический предел качества неперсонализированной спамовой фильтрации. ***Задача неперсонализированной программы – моделировать поведение максимально объективного незнакомого наблюдателя,*** не знающего ни про Ваши пристрастия, ни про Ваши подписки!
любом случае ключевой вопрос любой полноценной антиспам-системы состоит в решении, откуда брать сведения об ошибках первого и второго рода. Очевидно, что жалоба на спам или просьба о блокировке адреса – это обратная связь по ошибкам первого рода. Возможна и крайне желательна обратная связь и по ошибкам второго рода.

интерфейсе большинства современных публичных веб-почт (Hotmail, Yandex, Yahoo, Oddpost) есть специальная папка, служащая для накопления «полуспама» и не очень достоверно определяемого спама, а также кнопка для «реабилитации», сообщающая системе о ложном срабатывании. В настольных почтовых клиентах, созданных в последнее время, тоже обязательно присутствует обратная связь как первого, так и второго рода. Обычно в виде кнопки «это спам» / «это не спам».

Антивирусы способны:

1) обеспечивать защиту от вирусов, червей, троянских программ, различных вредоносных скриптов и кодов, распространяемых по каналам

электронной почты, через веб, интернетпейджеры, P2P-сети, мобильные устройства (карманные компьютеры и смартфоны);
определять и при необходимости блокировать активный код (Java-аплеты и элементы ActiveX);
обеспечивать защиту от представителей класса spyware;

предотвращать фишинг/фарминг-атаки.

Для решения последних двух задач антивирусное программное обеспечение, как правило, использует дополнительные утилиты, которые при необходимости включаются и настраиваются администратором безопасности заказчика.

Основным методом обнаружения вредоносных программ по-прежнему остается анализ сигнатуры проверяемых данных. Однако скорость распространения вредоносных программ гораздо выше скорости обновления антивирусных баз данных. На анализ нового вируса требуется определенное время. Поэтому ***от обнаружения новой вредоносной программы до выхода обновлений корпоративные сети остаются беззащитными. Выходом*** из данной ситуации ***является*** так называемый ***превентивный подход.***

Он включает в себя следующие методики обнаружения вредоносных программ.

Эвристический анализ. Анализ, основанный на поиске в исполняемых файлах отдельных записей кода, присущих вредоносным программам. Эвристический метод предназначен для выявления неизвестного вредоносного ПО. Хотя уровень обнаружения новых вирусов, червей и троянцев не превышает 25-30%, но эвристический анализ эффективен в сочетании с другими методами.

Анализ поведения программ. Анализируется последовательность действий вредоносной программы и блокируется выполнение любых опасных действий. (Например, блокировка отправки большого числа неавторизованных электронных сообщений лицам из адресной книги.) Возможно обнаружение любого типа вредоносного ПО. Имеет высокий уровень эффективности (до 70%).

Выявление формальных признаков вредоносной программы.
Для защиты почтового трафика могут использоваться методы, основанные на анализе почтовых сообщений, проходящих через почтовый сервер. С помощью такого анализа можно остановить эпидемию в самом ее начале. При этом к формальным признакам относятся: массовая рассылка или прием одинаковых вложений (одинаковых писем с различными вложениями),

наличие двойного расширения у вложений и т.п. Кроме того, возможен лингвистический анализ тел писем.

4. **Блокировка доступа пользователей к «запрещенным» Интернет-ресурсам.** Списки таких ресурсов составляются компаниями-производителями средств контентной фильтрации и антивирусных программ и распространяются по подписке.

При выборе антивирусных программ важно выяснить, могут ли они обнаруживать и удалять rootkit на Windows-системах. Для этого ***нужно многофункциональное антивирусное решение, способное работать с операционной системой на самых низких уровнях и контролировать все системные функции.***

Говоря о ***глубокой защите***, мы подразумеваем ***защиту системы на трех уровнях:***

обычные и удаленные пользователи, которых называют пользователями первого уровня;

файловые, принт-сервера, сервера приложений, базы данных, электронная почта, веб-сервера, которые называют устройствами второго уровня;

третий уровень или периметровые устройства, такие как, почтовые шлюзы, прокси-сервера, хосты VPN и другие точки соприкосновения с внешним миром.

Одна из самых тяжелых задач администратора безопасности - это очистка системы после заражения. После попадания злонамеренного кода в систему, он может находиться там продолжительное время и, в зависимости от антивирусного пакета, может пройти много времени, прежде чем администратор узнает, что система заражена. ***Используя два или более продукта на различных уровнях, вы повышаете шансы получить уведомление о заражении вовремя, что уменьшит время вашей реакции и предоставит информацию о проблеме от нескольких поставщиков.***

Наряду с традиционным сканированием на вирусы, ***настоящая глубокая защита подразумевает некоторые виды нетрадиционных методов***, например, фильтрацию содержимого.

Необходимо наличие контрольного центра и ответственного за защиту корпорации от вирусов. Назначая главных ответственных лиц, к тому же наделенных определенной властью, организация может установить процедуры для случаев заражения, и тогда можно с большей степенью уверенности утверждать, что распространение вируса будет приостановлено, а повреждения будут ликвидированы.

Глубокая защита - это больше чем защита каждого из уровней потенциального вторжения. Это согласованное использование лучших продуктов для каждой платформы, на каждом уровне систем организации, использование фильтров содержимого для снижения риска поражения нетрадиционным злонамеренным кодом, а также использование централизованной отчетности и выделение полномочий для управления стратегией антивирусной защиты. Единственным путѐм, обеспечивающим выполнение всех требований, остается эффективное обучение пользователей.

Практическое задание

Разработайте проект организации защищенного документооборота в соответствии с закрепленным предприятием.

Контрольные вопросы

Что такое защищенный документооборот?

Назовите основные компоненты необходимые для организации электронного документооборота.

Какие мероприятия необходимы для организации защищенного электронного документооборота?

Назовите основной метод обнаружения вредоносных программ.

Перечислите методики обнаружения вредоносных программ.

Лабораторная работа 14.

Изучение методов построения комплексной защиты сетевых приложений и баз данных

Цель работы: изучить методы построения комплексной защиты сетевых приложений и баз данных.

Теоретическая часть

Типовые архитектуры сетевых приложений

Сетевые приложения и базы данных тесно связаны между собой и являются ядром информационной инфраструктуры современного предприятия. Например, сетевую файловую систему можно рассматривать как сетевое приложение, использующее примитивную базу данных, записями которой являются файлы. В свою очередь, электронная почта также является сетевым приложением.

Сетевые базы данных обеспечивают распределенное хранение информационных ресурсов предприятия, а сетевые приложения — их распределенную обработку.

Под термином *«распределенный» мы,* прежде всего, *понимаем совместную работу взаимодействующих вычислительных устройств и средств телекоммуникаций, направленную на достижение общей цели, решение общей задачи,* т. е. *нельзя рассматривать процессы распределенной обработки и хранения информации как простую сумму вычислительных ресурсов.* В принципе распределенной обработки информации отражены важнейшие системные свойства, определяющие качественное изменение технологий обработки информации.

Первое системное свойство — взаимодействие компонентов системы распре-дезенной обработки и хранения информации. Узлы компьютерной сети специализируются на решении отдельных подзадач, в процессе работы над которыми активно обмениваются необходимыми им данными. Речь идет не о простом распараллеливании вычислительного процесса, а о его

глубинном перерождении. *Носитсзем идей нового подхода к организации вычислитезьного процесса является объектно-ориентированное программирование.*

Задача описывается в виде взаимодействующих объектов, а ее решение есть некоторое визируемое состояние системы объектов, отвечающее четко описанным критериям. В компьютерной сети каждый из объектов может быть представлен в виде самостоятельного вычислительного процесса, работающего на одном или нескольких узлах.

Второе системное свойство — масштабируемость системы распределенной обработки и хранения информации. Описание задачи в виде типовых элементарных объектов с детально описанными правилами взаимодействия позволяет легко наращивать производительность вычислительной системы и адаптировать ее к динамично меняющимся условиям и требованиям современного мира.

Третье системное свойство— независимость макроархитектуры системы распределенной обработки и хранения информации от микроархитектуры ее элементов. Данное свойство выражается в реализации взаимодействия компонентов через интерфейсы, определяющие функциональное содержание их ролей. Иначе говоря, системе нет никакого дела до внутренней реализации каждого интерфейса отдельными объектами, и эволюция вычислительных процессов в каждом объекте может протекать независимо от остальных элементов.

Простейшая архитектура сетевого приложения была описана в разделе, посвященном комплексной защите сетевой файловой системы. Она основывалась на расширении классического вызова подпрограммы, возможностью вызова процедуры, которая в действительности выполнялась на другом узле компьютерной сети. Сама сеть при этом служила для передачи идентификатора требуемой функции и параметров вызова, а после

окончания работы программы на удаленном узле — результатов ее выполнения.

Такая модель хорошо работала на заре эры компьютерных сетей и глобальных телекоммуникаций. Процесс укрупнения и усложнения информационных систем, который неотрывно следовал за аналогичными процессами в мировой экономике, вызвал эволюцию организации вычислительного процесса, и она пошла по тому же пути, что и в области классического программирования. На горизонте появились объекты.

Если раньше приложение разрабатывалось целиком от интерфейса пользователя до подсистемы хранения данных, то теперь эти задачи разделились, и работа над ними стала проводиться независимо. Совершенствование технологий разработки программного обеспечения позволило появиться такому направлению, как САБЕ-технологии.

Теперь программы можно строить из готовых блоков — объектов; необходимо только описать правила их взаимодействия. Именно этой цели и служат современные языки описания сценариев, которые включают в себя основные алгоритмические конструкции и средства оперирования объектами.

Структура объектов сетевого приложения приведена на рис. 1.1.

На схеме показано распределение объектов сетевого приложения по различным зонам.

Обратите внимание на то, что *объекты существуют в ОЗУ, ДЗУ и ЛВС во время выполнения приложения.* Программный код, реализующий методы объектов, хранится в ДЗУ до того момента, пока не будет загружен в ОЗУ и связан со структурой данных, описывающих атрибуты или поля объектов. Как и их предшественники — классические приложения, выполняемые на одном процессоре, вычислительном устройстве, — сетевые приложения могут использовать все возможности системы ввода/вывода. Но *наибольшую эффективность от использования сетевых приложений можно получить,*

если в качестве источника информации будут выступать сетевые базы данных.

Сетевые базы данных, как и сетевые приложения — это, прежде всего, распределенная система. Но если сетевые приложения специализируются на распределенной обработке данных, то сетевые базы данных — на распределенном хранении данных.

Задача распределенного хранения заключается не только в «распылении» данных по узлам компьютерной сети, но, прежде всего, в обеспечении их целостности и доступности. Не будет особой пользы от того, что «А» хранится здесь, а «Б» — на другом конце земного шара. А вот если требуемые нам данные извлекаются быстро из ближайшего к нам источника и при этом всегда поддерживаются в актуальном состоянии независимо от удаленности от первичного источника информации — это совсем другое дело.

*База данных— это модель некоторой предметной области, включающая в себя факты и логические отношения между ними.*С точки зрения формальной логики *процесс работы с базой данных — это процесс доказательства или опровержения теорем, некоторой теории, аксиомами которой являются факты {записи) базы данных, а правила вывода соответствуют классической логике высказываний или логике предикатов первого порядка.*

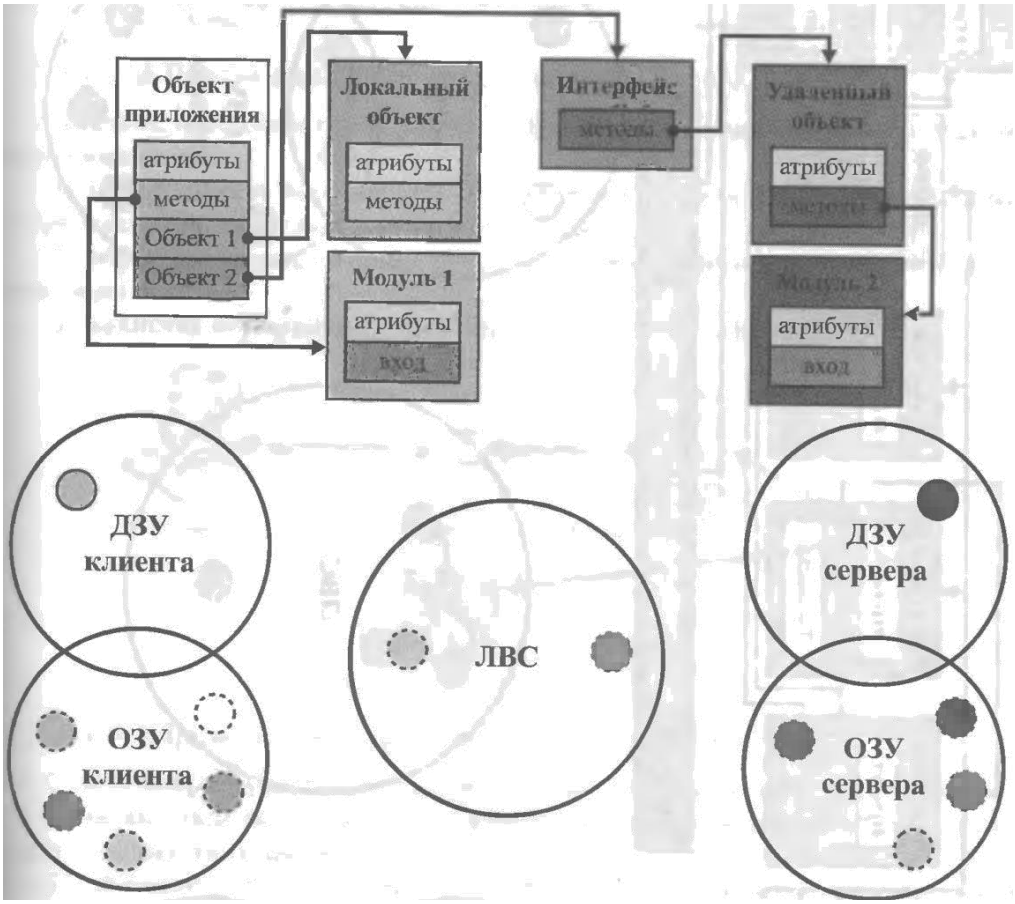


Рис. 1.1. Структура объектов сетевого приложения

Наибольшая концентрация объектов наблюдается в оперативной памяти сервера баз данных.

Давайте посмотрим на типовые архитектуры построения современных сетевых приложений, использующих в качестве основного источника информации сетевые базы данных

В схеме приложение выполняется на компьютере пользователя и взаимодействует посредством компьютерной сети с сервером баз данных. Это наиболее простая схема организации сетевого приложения, где на сеть ложится нагрузка по передаче информации между приложением и базой данных.

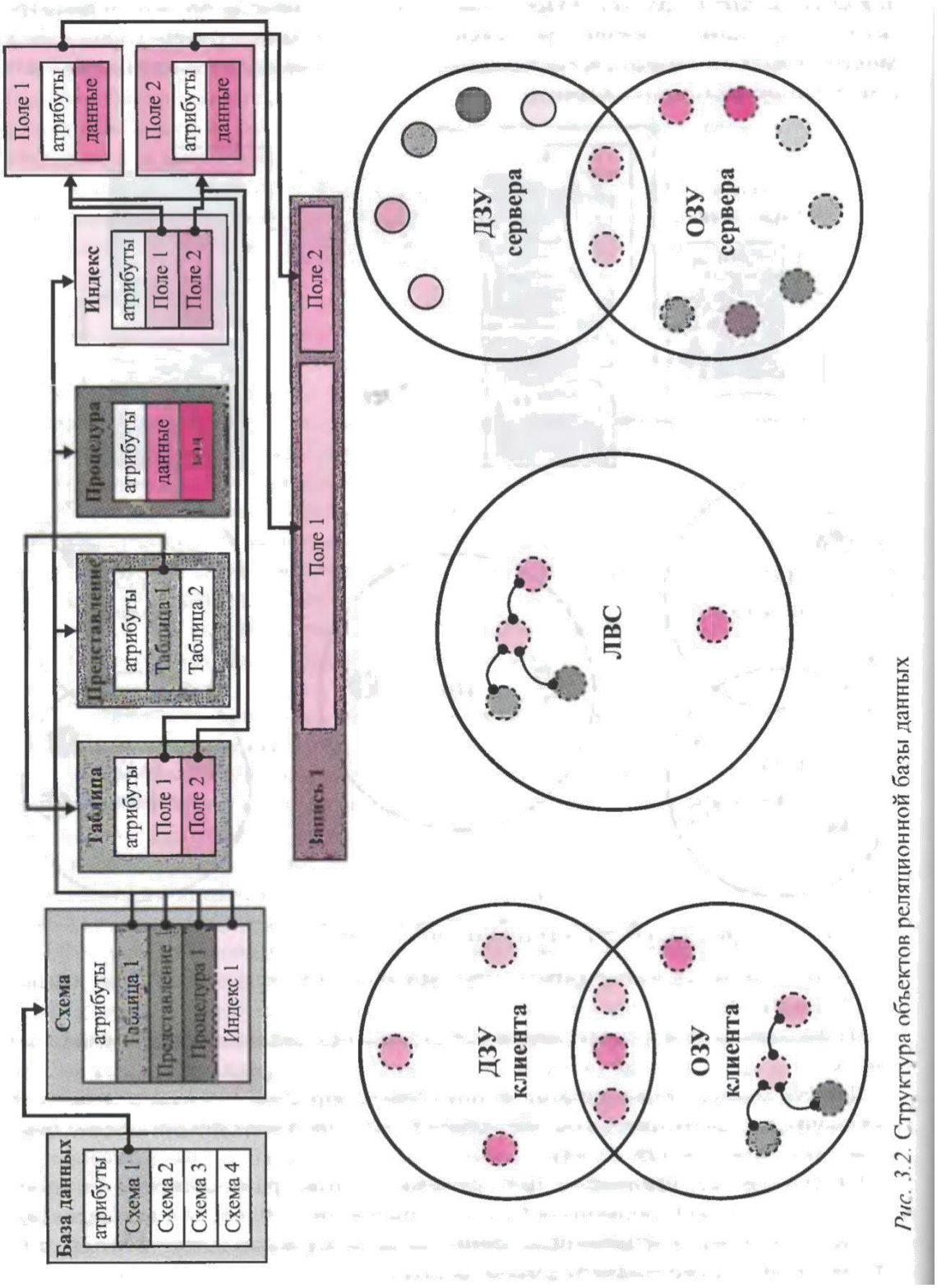


Рис. 3.2. Структура объектов реляционной базы данных

Рис. 1.2.Структура объектов реляционной базы данных

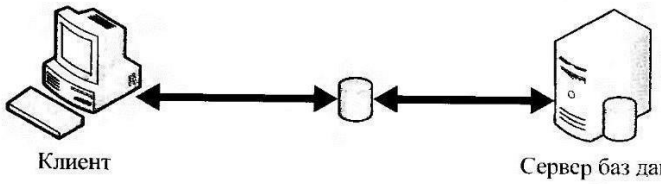


Рис. 1.3. Простая схема организации сетевого приложения

На схеме, показанной на рис. 1.4, *мы наблюдаем декомпозицию задачи на три независимых процесса:*
представление информации — реализуется программными средствами сетевого приложения, выполняемыми на компьютере клиента;
обработка информации— реализуется программным обеспечением сервера приложения;
хранение информации — реализуется сервером базы данных.

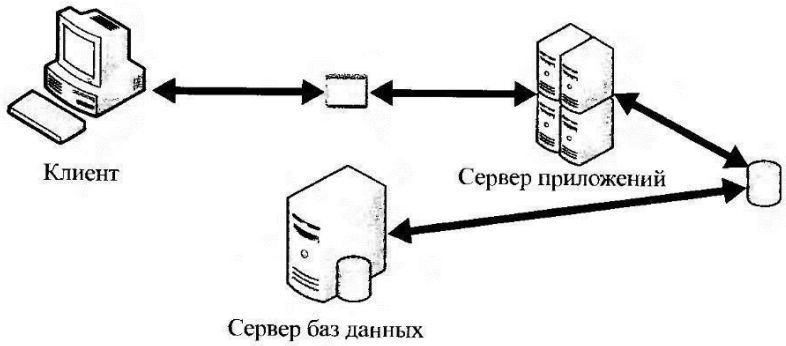


Рис. 1.4. Три независимых процесса в сетевом приложении

Главными преимуществами такой архитектуры приложения являются: независимая эволюция каждого компонента, которая может происходить в разное время с различной скоростью;
повышение производительности за счет специализации и оптимизации каждого вычислительного устройства на решении узкой, относительно самостоятельной задачи;
неограниченное наращивание возможностей за счет использования типовых элементов и правил их взаимодействия.
Пример наращивания возможностей сетевого приложения, использующего сетевые базы данных, показан на рис. 1.5.
Отличие представленной на рис. 1.6 архитектуры от предыдущей заключается в разделении задачи представления информации между клиентом сетевого приложения иWeb-сервером. *Это позволяет отказаться от необходимости устанавливать на клиенте компьютера дополнительное*

программное обеспечение, предназначенное для организации взаимодействия с *сервером приложения.*

Вместо этого используется унифицированный клиент на базе обозревателя 1пгете1 и стандартный протокол HTTP. Web-сервер переводит зависящие от приложения элементы представления информации на язык стандартных примитивов, описываемых языком HTML, на смену которому в последнее время приходит более современный и удобный стандарт XML. Web-сервер выполняет «отрисовку» электронного документа, который можно сохранить на носителе пользователя, вывести на печать или отправить по электронной почте. В то же время Web-сервер унифицирует процедуру взаимодействия пользователя через интерфейс форм, позволяющих структурировать запрос пользователя к информационной системе.

Рис. 1.5. Наращивание возможностей сетевого приложения

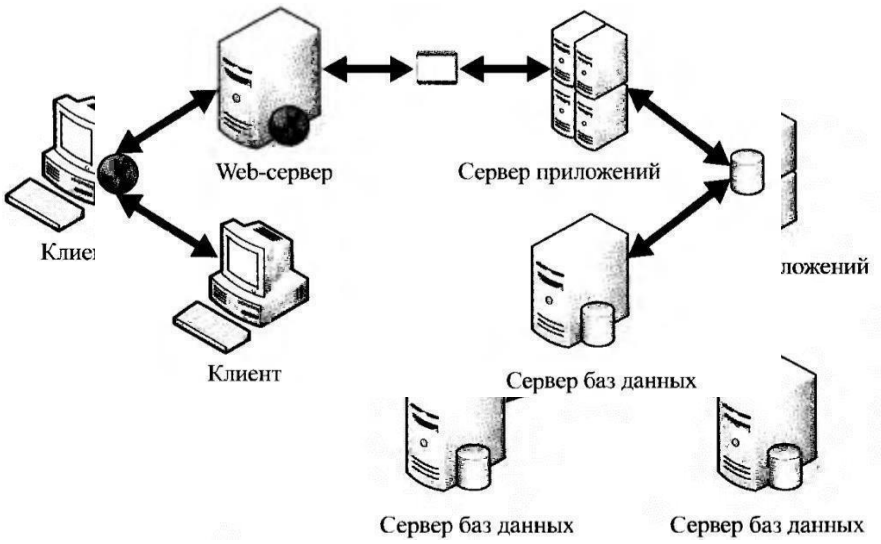


Рис. 1.6. Разделение задачи представления информации между клиентом сетевого приложения и Web-сервером.

Задачу сопряжения интерфейса сетевого приложения и интерфейса унифицированного клиента выполняют Web-приложения. Это сценарии, оперирующие объектами и выполняющие отображение множества параметров сетевого приложения на множество элементов управления унифицированного клиента.

Но даже такой гибкой архитектуры оказалось недостаточно для удовлетворения потребности в удобной и эффективной разработке сетевых приложений любой сложности.

Поэтому в настоящий момент используется более сложная схема, показанная на рис. 1.7.

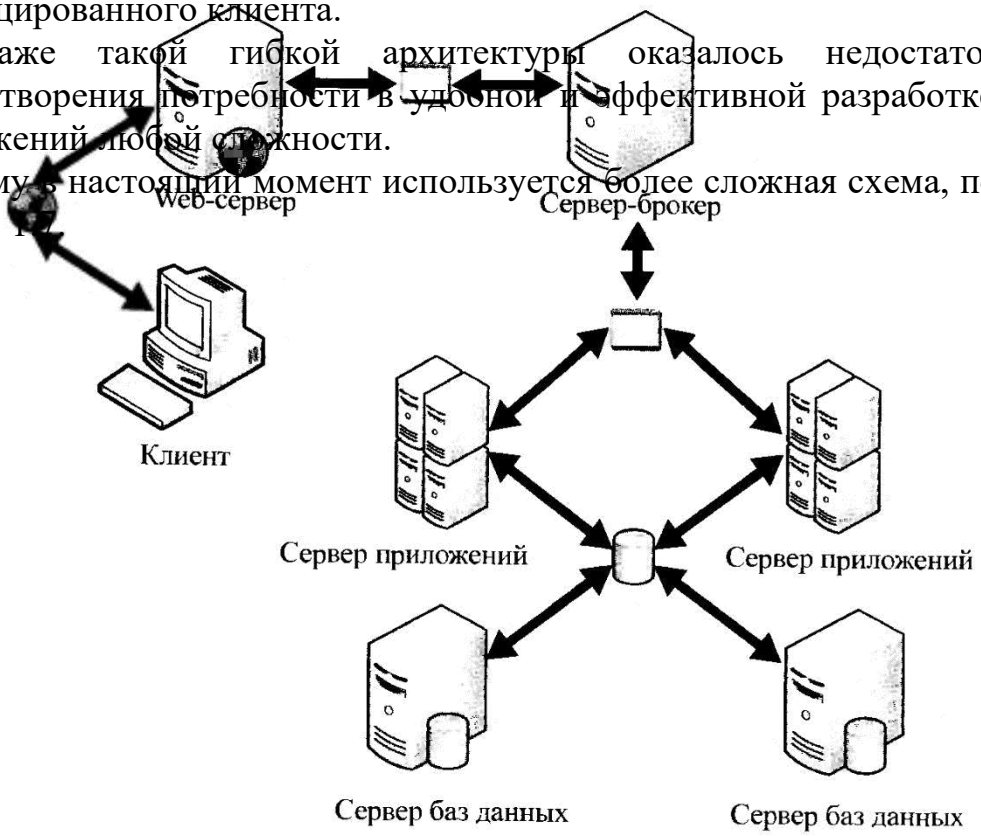


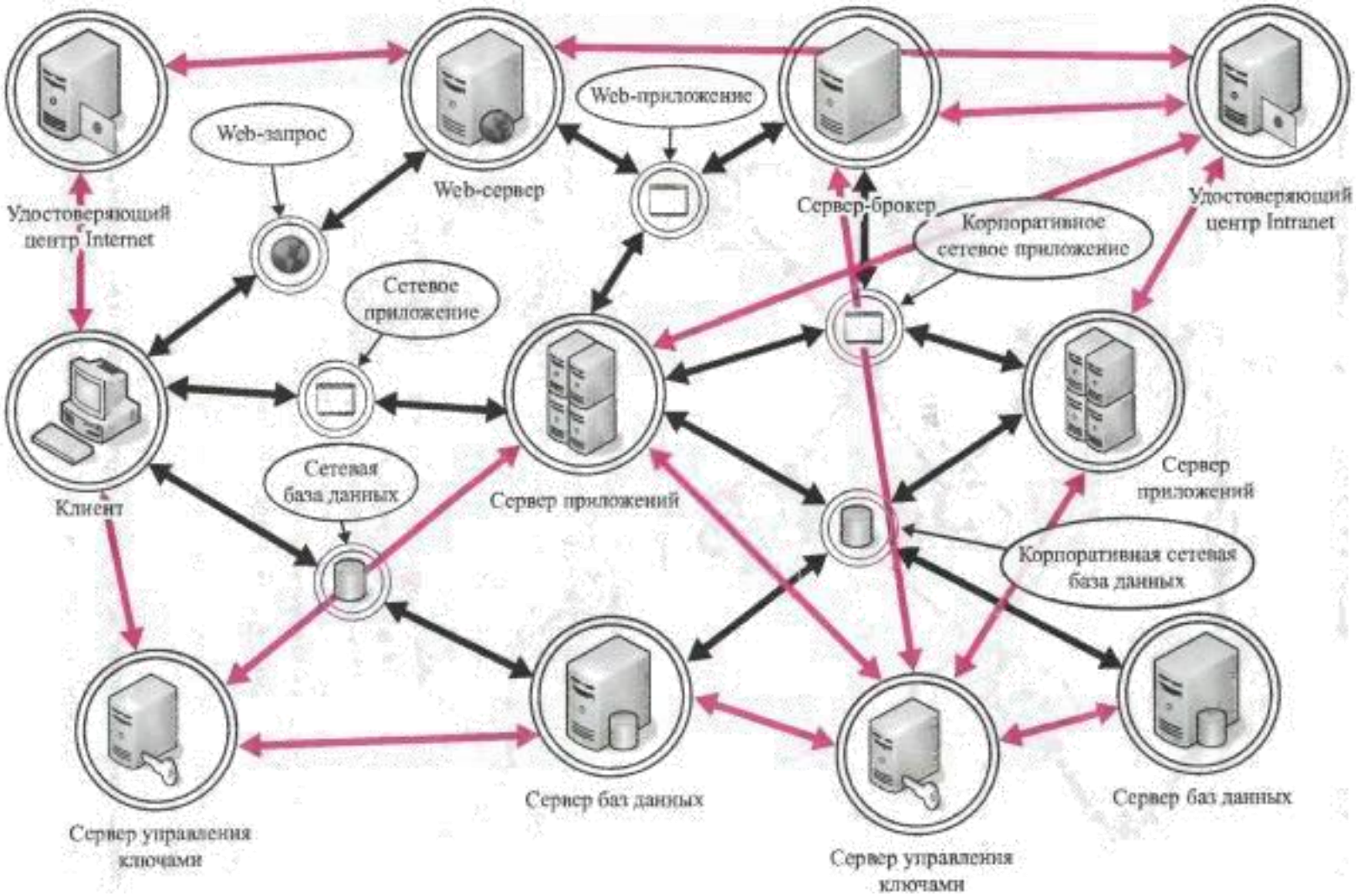
Рис. 1.7. Архитектура сетевого приложения с сервером-брокером.

В архитектуру добавлен сервер-брокер, задача которого — поиск необходимых для работы сетевого приложения объектов на одном или более серверах приложений. Введение этого компонента повышает эффективность работы сетевого приложения, упрощает «сборку» объектов приложения, поскольку теперь нет необходимости учитывать топологию серверов приложений, местонахождение отдельных объектов, требуемых для решения задачи. Мы просто сообщаем серверу-брокеру, что нам нужно, а он, в свою очередь, основываясь на оперативной информации о доступных ему ресурсах, выбирает оптимальный путь решения нашей проблемы. Теперь объекты сетевых приложений могут свободно мигрировать между серверами для достижения наибольшей производительности, и это никак не скажется на работе сетевых приложений, поскольку в функции сервера-брокера входит отслеживание всех изменений в размещении компонентов приложения.

Все рассмотренные схемы успешно сосуществуют в мире современных сетевых приложений.

Комплексная защита сетевых приложений и баз данных

Перейдем к рассмотрению комплексной защиты сетевых приложений и баз данных (рис. 1.8).


Web-запрос
Web-приложение
Web-сервер
Сервер-брокер
Удостоверяющий центр Internet
Удостоверяющий центр Intranet
Корпоративное сетевое приложение
Сетевое приложение
Клиент
Сервер приложений
Сервер приложений
Сетевая база данных
Корпоративная сетевая база данных
Сервер управления ключами
Сервер баз данных
Сервер баз данных
Сервер управления ключами

Выполним разбиение на отдельные контуры зашиты. Начнем с рассмотрения различных зон ЛВС (рис. 1.9).

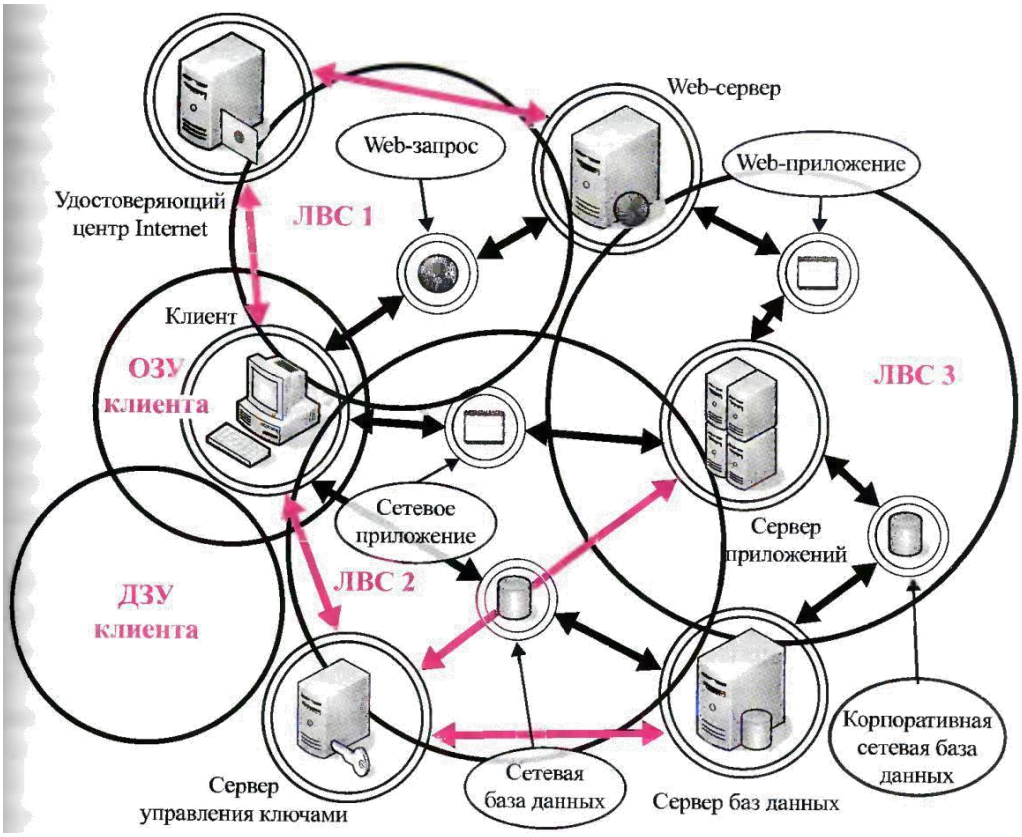


Рис. 1.9. Различные зоны ЛВС

Обратите внимание на три различные зоны ЛВС: ЛВС 1, ЛВС 2 и ЛВС 3. Зона ЛВС 1 относится к фрагменту телекоммуникационной системы, связующей клиента сетевого приложения и Web-сервер, обслуживающий представительскую логику. *Здесь речь идет, в том числе, и об участке, проходящем в системе глобальных телекоммуникаций*. В случае Intranet данная зона пересекается с зоной ЛВС 2. Это локальная вычислительная сеть, в которую непосредственно включены и клиент сетевого приложения, и серверы.

Зона ЛВС 3 *соответствует защищенному или изолированному участку корпоративной сети, обслуживающей серверы информационных служб и приложений.*

Она может пересекаться с зоной ЛВС 2 локальной вычислительной сети какого-либо подразделения, но, как правило, не пересекается с зоной ЛВС 1 — зоны глобальных телекоммуникаций.

Рассматриваемый контур защиты описывает рубежи и средства защиты информации, непосредственно взаимодействующие с клиентской составляющей сетевого приложения.

В зоне ДЗУ клиента сетевого приложения, согласно схем объектов защиты, содержатся: фрагменты баз данных, доступ к которым осуществляется в текущем сеансе, и которые были сохранены (кэшированы) на жестком диске компьютера в целях повышения производительности или избегания ненужных повторных передач информации, которая мало подвержена изменениям; модули объектов сетевого приложения; электрон-ные документы, полученные в результате работы сетевого приложения.*Особый интерес для злоумышленников представляют файлы конфигурации* (*настроек*) *сетевых приложений*, которые могут содержать критическую информацию — реквизиты доступа к серверам баз данных или серверам приложений.

Типовые нападения на зону ДЗУ клиента:

несанкционированный доступ к временным файлам с фрагментами баз данных и электронных документов; цель: располагая информацией об архитектуре и особенностях реализации сетевого приложения, получить доступ к классифицированной информации, незащищенной средствами сетевого приложения;

хищение модулей и файлов конфигурации сетевых приложений; цель: используя возможности файловой системы, выполнить копирование модулей и файлов конфигурации сетевого приложения на носитель злоумышленника для последующего анализа на предмет наличия уязвимостей и возможностей получения несанкционированного доступа к информационным ресурсам сетевого приложения;

модификация модулей и файлов конфигурации сетевых приложений; цель: ослабить или обойти средства защиты информации сетевого приложения для

последующего создания удобного плацдарма, с которого можно осуществить доступ к информационным ресурсам сетевого приложения;
внедрение программных закладок в программное обеспечение сетевых приложений; цель: установление контроля над вычислительными средствами клиента сетевого приложения в момент его запуска санкционированным пользователем.
Основной рубеж защиты создается с помощью встроенных средств защиты информации операционной системы и сетевого приложения. *На первый план выходят средства контроля целостности и криптографической защиты информации.* Привлечение средств электронной цифровой подписи позволяет ужесточить контроль за внесением изменений в программную среду клиента сетевого приложения. Качественная настройка механизмов операционной системы позволяет создать изолированное окружение для программного обеспечения сетевого приложения — так называемую «песочницу». Суть данного подхода заключается в ограничении сетевого приложения в выполнении потенциально опасных операций: запись в привилегированные области файловой системы, запуск новых процессов, загрузка исполняемых модулей и т. п. *Управление средствами защиты сетевых приложений строится на основе системы правил политики безопасности сетевого приложения.* Разработчики платформ для сетевых приложений предоставляют удобные графические и интуитивно понятные интерфейсы для настройки таких механизмов.
Зоне ОЗУ клиента сетевого приложения угрожают следующие типовые нападения:
использование уязвимостей программного обеспечения сетевого приложения; цель: путем перехвата управления внедрить в исполняемые процессы вредоносноепрограммное обеспечение с последующим проникновением его в зону ДЗУ и имплантацией в программную среду вычислительной системы;

хищение реквизитов доступа к сетевым базам данных и приложениям; цель: обнаружить в оперативной памяти структуры, содержащие критическую информацию — реквизиты доступа пользователя,
перенести ее в область, потенциально доступную злоумышленнику; реализуется через программные закладки и уязвимости программного обеспечения;
подключение к существующему сеансу работы с базой данных или сетевым приложением; цель: захватить контроль над рабочими объектами сетевых приложений, как правило, копированием или созданием ссылки на объекты интерфейсов доступа к базе данных или сетевому приложению после процедуры аутентификации и согласования параметров безопасности;
перехват электронных документов; цель: используя архитектурные особенности унифицированных клиентов сетевых приложений (например стандартного обозревателя 1п1еше1), получить доступ к классифицированной информации в виде электронных документов, «осевших» в накопительных областях (кэшах);
подмена загружаемых модулей; цель: вынудить клиентское программное обеспечение выполнить загрузку исполняемого модуля, навязанного злоумышленником;
нарушение работы сетевого приложения; цель: посредством уязвимостей или, используя архитектурные особенности сетевого приложения, частично или полностью вывести его из строя;
7) навязывание операций; цель: используя уязвимости программного обеспечения, архитектурные особенности или программные закладки, выполнить имитацию операций санкционированного пользователя.
Основной рубеж защиты создается взаимодействием встроенных средств зашиты операционной системы, программного обеспечения сетевого приложения и специальными программными средствами защиты:

антивирусные программы, персональные межсетевые экраны, программы создания изолированных сред или виртуальных вычислительных систем, программы обнаружения вторжений, программы автоматического поиска уязвимостей.

Зоны ЛВС 1, ЛВС 2, ЛВС 3 подвержены следующим типовым нападениям: перехват данных; цель: восстановить информационные объекты из перехваченных сетевых пакетов с последующим извлечением ценной информации на вычислительных средствах злоумышленника;

ложный сервер: цель: активно подавляя санкционированный сервер, вынудить клиента сетевого приложения к работе с сервером злоумышленника; данное нападение позволяет похитить реквизиты доступа к санкционированному серверу или навязать ложную информацию пользователю сетевого приложения:

блокирование клиента сетевого приложения; цель: используя уязвимости программного обеспечения, особенности архитектуры и топологии телекоммуникационной системы, прекратить работу сетевого приложения; внедрение в сеанс работы сетевого приложения; цель: используя подконтрольные злоумышленнику средства телекоммуникации модифицировать канал передачи данных, внедрив в него промежуточный сетевой узел, который по отношению к клиенту выступает в роли сервера, а по отношению к серверу — в роли клиента.

Отражение нападений реализуется средствами сетевых операционных систем, встроенными средствами сетевых приложений, аппаратно-программными средствами межсетевых экранов и телекоммуникационного оборудования. Для контроля целостности и защиты конфиденциальности данных применяются криптографические средства. Взаимную аутентификацию клиента и сервера необходимо проводить на основе инфраструктуры открытого ключа особенно для зоны ЛВС 1. В зонах ЛВС 2 и ЛВС 3 допустимо использовать централизованный сервер управления ключевой

информацией и скоростные алгоритмы шифрования информации на основе симметричной криптографии.

Для раннего обнаружения и предотвращения нападений на ресурсы сетевых приложений и баз данных применяются системы обнаружения вторжений и автоматического поиска уязвимостей. Сенсоры данных систем, расположенные в соответствующих зонах, дополнительно могут быть усилены сенсорами, размещенными в сетевых узлах. Борьба с вредоносным программным обеспечением ведется с помощью кор-поративных программных средств антивирусной защиты и контроля целостности.

Рубежи криптографической защиты в сетевых зонах реализуются взаимодействием криптографических средств операционных систем, сетевых приложений, межсетевых экранов и телекоммуникационного оборудования. Данные средства обеспечивают глубокоэшелонированную криптографическую защиту передаваемой информации.

Защита процедур взаимодействия средств представления информации со средствами ее обработки

Данный контур защиты описывает взаимодействие средств представления информации со средствами ее обработки (рис. 1.10).

Web-приложения, которые реализуются, как правило, в виде сценариев, описывающих операции над системными и пользовательскими объектами, осуществляют доступ к ресурсам сервера-брокера или сервера приложений. Объектом взаимодействия этих трех подсистем является, прежде всего, адресная информация о расположении фрагментов приложения.

Зоне ДЗУ Web-сервера угрожают следующие типовые нападения:

модификация сценариев Web- приложений; цель: используя уязвимости программного обеспечения, ошибки конфигурации и программные закладки, внедрить в сетевое приложение объекты злоумышленника;

модификация модулей программного обеспечения и файлов конфигураций Web-сервера; цель: используя уязвимости программного обеспечения, ошибки конфигурирования или программные закладки, получить контроль над Web-сервером;
хищение реквизитов доступа из файлов конфигурации; цель: извлечь или восстановить из файлов конфигурации \\'еЬ- приложения критическую информацию, позволяющую получить доступ к серверу приложений или серверу-брокеру от лица санкционированного пользователя.

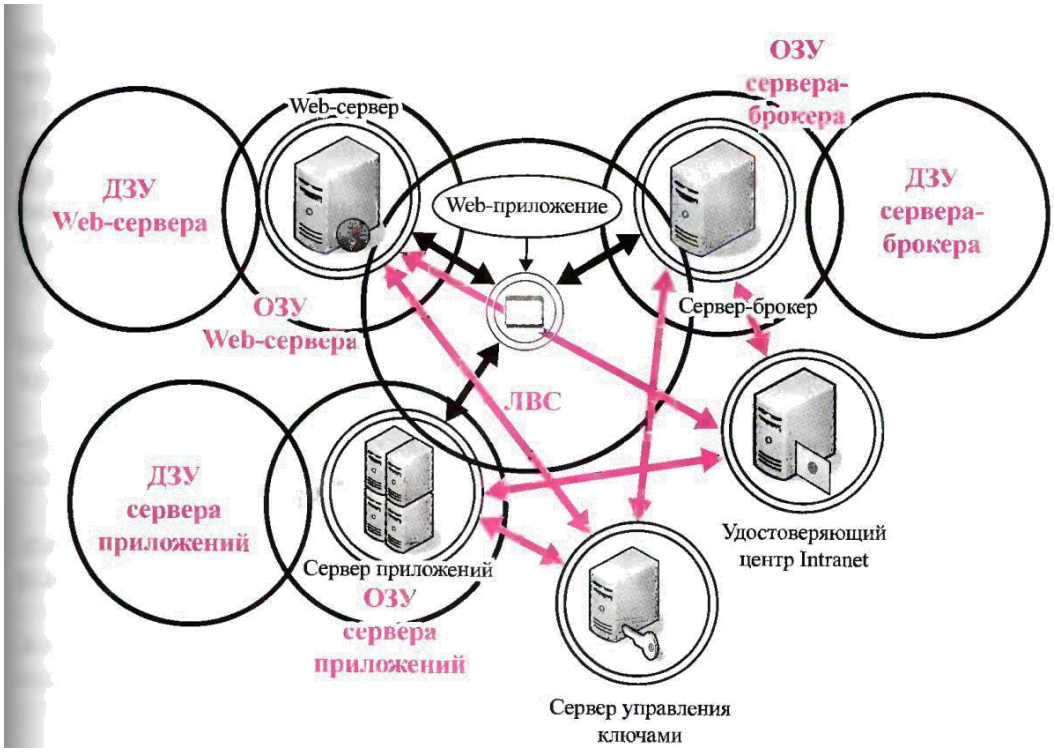


Рис. 1.10. Взаимодействие средств представления информации со средствами ее обработки

Зона ОЗУ Web-сервера подвержена следующим нападениям:
использование уязвимостей программного обеспечения; цель: захват контролянад Web-сервером через уязвимости программного обеспечения, ошибки конфигурации или внедрение программных закладок;

навязывание логики обработки запроса пользователя; цель: через манипуляцию параметрами и использование служебных функций программного обеспечения Web-сервера модифицировать логику обработки запроса пользователя в интересах злоумышленника;
исчерпание ресурсов Web-сервера — отказ в обслуживании; цель: используя уязвимости программного обеспечения, ошибки конфигурации и программные закладки в короткое время исчерпать свободные ресурсы web-сервера и, тем самым, нарушить работу по обслуживанию пользователей;
перехват объектов доступа к сетевым базам данных и приложениям; цель: используя отладочные функции операционных систем и специальные методы программирования, получить доступ к объектам времени выполнения, созданным после процедур аутентификации и авторизации пользователя, позволяющим выполнять операции с сетевыми приложениями и базами данных от его лица.

Типовые нападения на зону ДЗУ сервера приложений:
модификация программных модулей и файлов конфигурации
сетевых приложений; цель: используя прямой доступ к носителю информации, злоумышленник модифицирует или полностью заменяет программные модули и файлы конфигураций сетевых приложений для достижения своих целей;
хищение реквизитов доступа к сетевым базам данных и серверам приложений; цель: извлечение или восстановление критической информации из программных модулей и файлов конфигураций сетевых приложений, содержащей идентификаторы и аутентификаторы санкционированных пользователей.

Типовые нападения на зону ОЗУ сервера приложений:

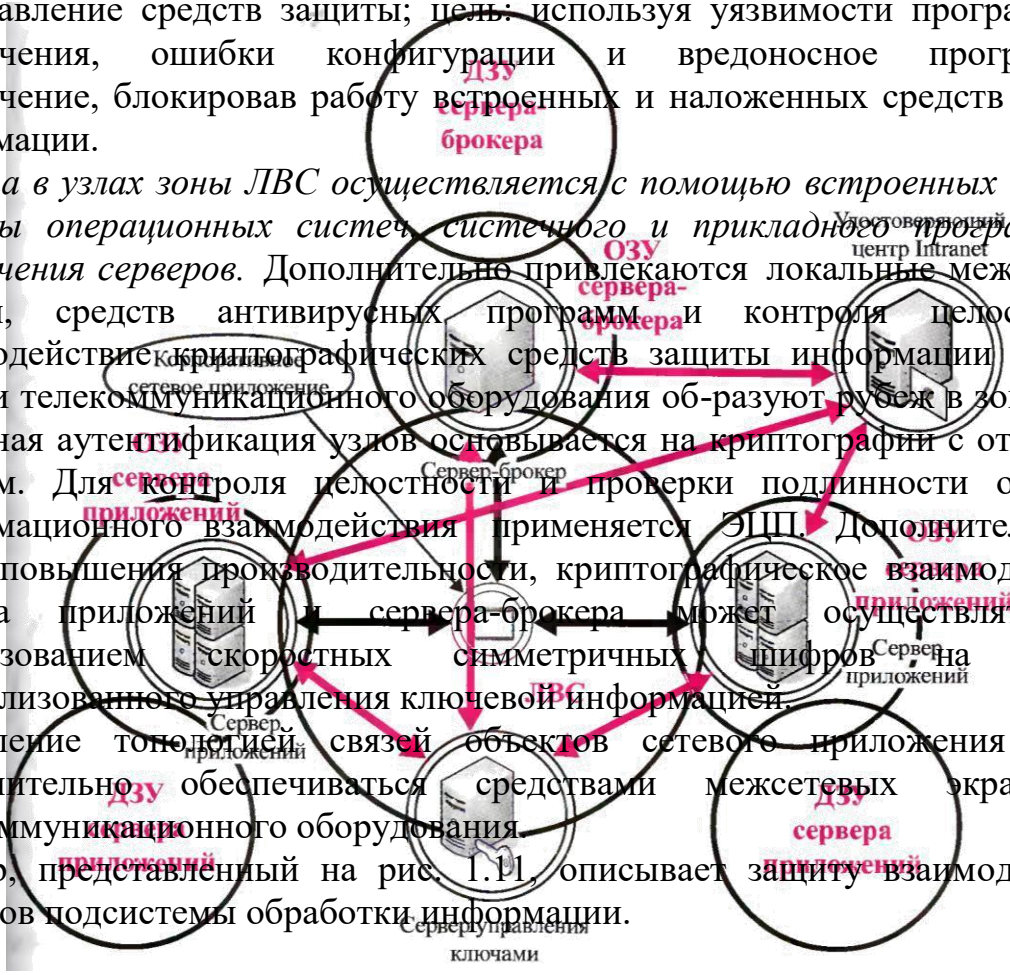
использование уязвимостей программного обеспечения; цель: установление контроля над сервером приложений путем воздействия на уязвимости программного обеспечения и ошибки конфигурации;
внедрение в активный сеанс сетевого приложения; цель: обойти средства аутентификации и авторизации и воспользоваться активными структурами существующего сеанса для осуществления доступа от лица санкционированного пользователя;
подавление средств защиты; цель: используя архитектурные особенности реализации, уязвимости встроенных и прицепных средств защиты, вывести их из строя или снизить эффективность;
модификация активных объектов; цель: используя программные закладки, обойти средства контроля целостности сетевых приложений и выполнить модификацию программного кода в оперативной памяти в интересах злоумышленника.
Типовые нападения на зону ДЗУ сервера-брокера:
модификация исполняемых модулей и файлов конфигурации сервера-брокера; цель: путем модификации программного обеспечения или файлов конфигурации установить контроль над сервером-брокером;
модификация базы данных размещения объектов сетевых приложений. цель: изменить топологию связей объектов сетевого приложения, внедрить объекты злоумышленника.
Типовые нападения на зону ОЗУ сервера-брокера:
использование уязвимостей программного обеспечения; цель:

воздействуя н.; уязвимости программного обеспечения, ошибки конфигурации или внедряя программные закладки, установить контроль над сервером-брокером в интересах злоумышленника;
имитация события изменения расположения объектов сетевого
приложения; цель: ввести в базу данных сервера-брокера ложную

информацию о расположении объектов сетевого приложения в узлах компьютерной сети;

3) подавление средств защиты; цель: используя уязвимости программного обеспечения, ошибки конфигурации и вредоносное программное обеспечение, блокировав работу встроенных и наложенных средств защиты информации.

Защита в узлах зоны ЛВС осуществляется с помощью встроенных средств защиты операционных систем, системного и прикладного программного обеспечения серверов. Дополнительно привлекаются локальные межсетевые экраны, средств антивирусных программ и контроля целостности. Взаимодействие криптографических средств защиты информации сетевых узлов и телекоммуникационного оборудования об-разуют рубеж в зоне ЛВС. Взаимная аутентификация узлов основывается на криптографии с открытым ключом. Для контроля целостности и проверки подлинности объектов информационного взаимодействия применяется ЭЦП. Дополнительно, в целях повышения производительности, криптографическое взаимодействие сервера приложений и сервера-брокера может осуществляться с использованием скоростных симметричных шифров на основе централизованного управления ключевой информацией.



Управление топологией связей объектов сетевого приложения может дополнительно обеспечиваться средствами межсетевых экранов и телекоммуникационного оборудования.

Контур, представленный на рис. 1.11, описывает защиту взаимодействия объектов подсистемы обработки информации.

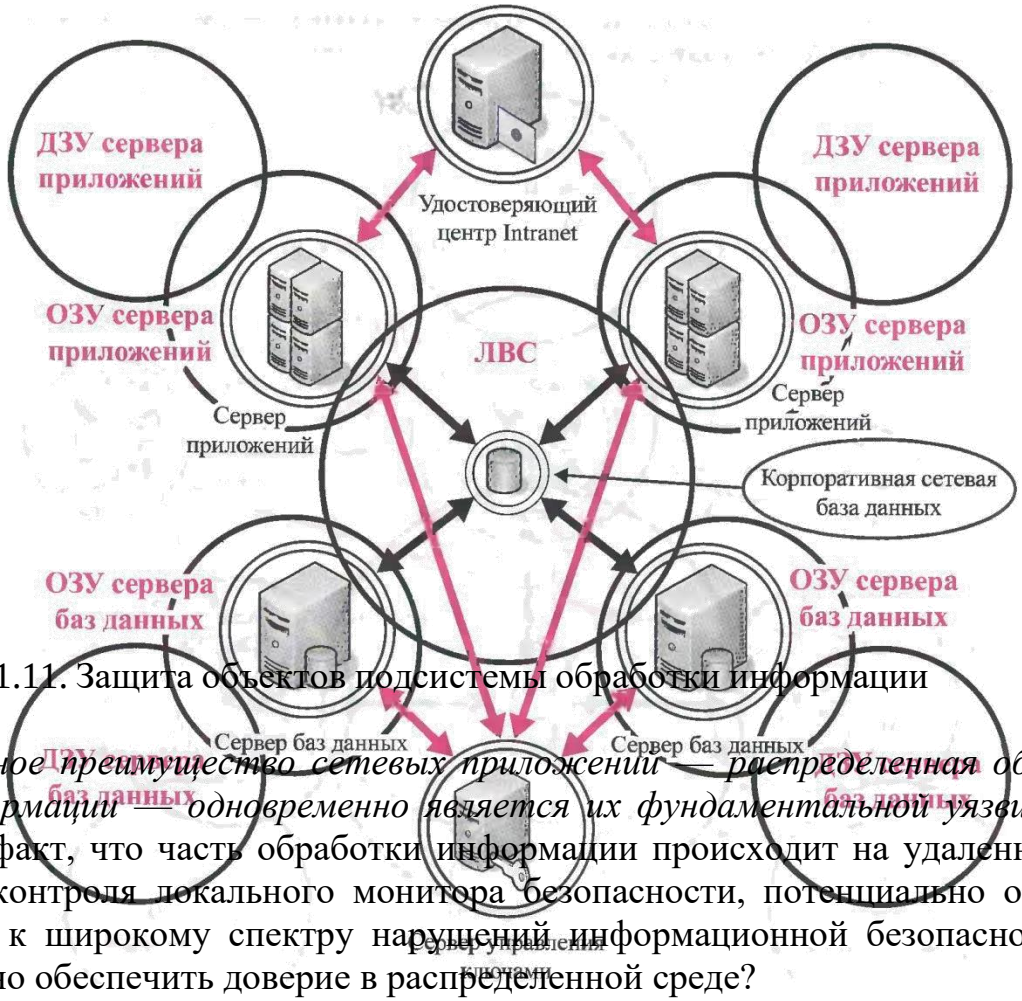


Рис. 1.11. Защита объектов подсистемы обработки информации

Главное преимущество сетевых приложений — распределенная обработка информации — одновременно является их фундаментальной уязвимостью. Тот факт, что часть обработки информации происходит на удаленном узле, вне контроля локального монитора безопасности, потенциально открывает путь к широкому спектру нарушений информационной безопасности. Как можно обеспечить доверие в распределенной среде?

Прежде всего, *жестким контролем над информационными потоками,*

который реализуется аппаратно-программными средствами межсетевых экранов и телекоммуникационного оборудования. И, конечно, немыслимо обойтись без средств криптографической защиты.

Рис. 1.12. Защита взаимодействия подсистемы обработки информации с подсистемой хранения

Принцип спецслужб: доверяй, но проверяй, активно используется при распределенной обработке информации. Загружаемые исполняемые модули проверяются на наличие в них запрещенных политикой безопасности операций. Для них вводятся ограничения по доступу к привилегированным объектам операционной системы и программной среды серверов приложений. Входные данные контролируются на предмет соответствия типов, принадлежности к допустимому диапазону значений, выполнения логических условий, наличия известных признаков информационных нападений. Выходные данные также проверяются на соответствие типов, диапазонов значений, выполнение логических условий, в том числе связанных с информационной безопасностью. Использование ключевых

параметров в системах криптографической защиты строго лимитировано по времени.

Остановимся на типовых нападениях, характерных для зоны ЛВС:

перехват данных; цель: восстановить из перехваченных сетевых пакетов сеансы удаленного вызова процедур и функций, а также извлечь информацию о переданных дтя обработки и полученных после нее данных; внедрение в сеанс; цель: активно подавляя одного из участников сеанса, после того как были завершены фазы аутентификации и авторизации, занять его место в сетевом сеансе и получить доступ к информационным ресурсам и услугам;
блокирование сетевых приложений: цель: используя архитектурные особен-шости. уязвимости и ошибки конфигурации, нарушить штатное функционирование сетевых приложений.
Контур, представленный на рис. 1.12, описывает защиту взаимодействия подсистемы обработки информации с подсистемой хранения.

Защита информации в базах данных

В современных СУБД поддерживается один из двух наиболее общих подходов к вопросу обеспечения безопасности данных: *избирательный подход и обязательный подход.* В обоих подходах единицей данных или «объектом данных», для которых должна быть создана система безопасности, может быть как вся база данных целиком, так и любой объект внутри базы данных.
Эти два подхода отличаются следующими свойствами:
в случае избирательного управления некоторый пользователь обладает различными правами (привилегиями или полномочиями) при работе с данными объектами. Разные пользователи могут обладать разными правами доступа к одному и тому же объеду. Избирательные права характеризуются значительной гибкостью;

в случае избирательного управления, наоборот, каждому объекту данных присваивается некоторый классификационный уровень, а каждый пользователь обладает некоторым уровнем допуска. При таком подходе доступом к определенному объекту данных обладают только пользователи с соответствующим уровнем допуска;

для реализации избирательного принципа предусмотрены следующие методы. 6 базу данных вводится новый тип объектов БД — это пользователи. Каждому пользователю в БД присваивается уникальный идентификатор. Для дополнительной защиты каждый пользователь, кроме уникального идентификатора, снабжается уникальным паролем, причем если идентификаторы пользователей в системе доступны системному администратору, то пароли пользователей хранятся, чаше всего, в специальном кодированном виде и известны только самим пользователям;

пользователи могут быть объединены в специальные группы пользователей. Один пользователь может входить в несколько групп. В стандарте вводится понятие группы РОВиС, для которой должен быть определен минимальный стандартный набор прав. По умолчанию предполагается, что каждый вновь создаваемый пользователь, если специально не указано иное, относится к группе РСВЫС;

привилегии или полномочия пользователей или групп— это набор действий (операций), которые они могут выполнять над объектами БД;

в последних версиях ряда коммерческих СУБД появилось понятие «роли». *Роль — это поименованный набор полномочий.* Существует ряд стандартных ролей, которые определены в момент установки сервера баз данных. Имеется возможность создавать новые роли, группируя в них произвольные полномочия. *Введение ролей позволяет упростить управление привилегиями пользователей, структурировать этот процесс.* Кроме того,

введение ролей не связано с конкретными пользователями, поэтому роли могут быть определены и сконфигурированы до того, как определены пользователи системы;

пользователю может быть назначена одна или несколько ролей;
объектами БД, которые подлежат защите, являются все объекты, хранимые в БД- таблицы, представления, хранимые процедуры и триггеры. Для каждого типа объектов есть свои действия, поэтому для каждого типа объектов могут быть определены разные права доступа.
На самом элементарном уровне концепции обеспечения безопасности баз данных исключительно просты. *Необходимо поддерживать два фундаментальных принципа: проверку полномочий и проверку подлинности* (аутентификацию).
Проверка полномочий основана на том. что каждому пользователю или процесс) информационной системы соответствует набор действий, которые он может выполню I по отношению к определенным объектам. Проверка подлинности означает достоверное подтверждение того, что пользователь или процесс, пытающийся выполнить санкционированное действие, действительно тот, за кого он себя выдает.
Система назначения полномочий имеет в некотором роде иерархический характер Самыми высокими правами и полномочиями обладает системный администратор ил? администратор сервера БД. Традиционно только этот тип пользователей может создана! других пользователей и наделять их определенными полномочиями. СУБД в своих системных каталогах хранит как описание самих пользователей, так и описание их привилегий по отношению ко всем объектам.
Далее схема предоставления полномочий строится по следующему принципу. Каждый объект в БД имеет владельца — пользователя, который создал данный объект. Владелец объекта обладает всеми правами-

полномочиями на данный объект, в том числе и он имеет право предоставлять другим пользователям полномочия по работе с данным объектом или забирать у пользователей ранее предоставленные полномочия.
ряде СУБД вводится следующий уровень иерархии пользователей — администратор БД. В этих СУБД один сервер может управлять множеством СУБД (например MSSQLServer? Sybase).
СУБД Oracle применяется однобазовая архитектура, поэтому там вводится понятие подсхемы — части общей схемы БД, и вводится пользователь, имеющий доступ к подсхеме.
стандарте SQL определены два оператора: GRANT и REVOKE, соответственно предоставления и отмены привилегий.
Оператор предоставления привилегий имеет следующий формат:
GRANT {<списокдействий>| ALL PRIVILEGES }
ON <имя_объекта> TO {<имя_пользователя> | PUBLIC }
[WITH GRANT OPTION]
Здесь список определяет набор действий из общедопустимого перечня действий над объектом данного типа:
параметр ALL PRIVILEGES указывает, что разрешены все действия из допустимых хтя объектов данного типа;
<имя_объекта> задает имя конкретного объекта: таблицы, представления, хранимой процедуры, триггера;
<имя пользоватсля> или PUBLIC определяет, кому предоставляются данные привилегии:
параметр WITH GRANT OPTION является необязательным и определяет режим, при котором передаются не только права на указанные действия, но и право передавать эти права другим пользователям. Передавать права в этом случае пользователь может только в рамках разрешенных ему действий.

Рассмотрим пример. Пусть у нас существуют три пользователя с абсолютно уникальными именами userl, user2 и user3. Все они являются пользователями одной БД.

Userl создал объект Tab1; он является владельцем этого объекта и может передать права на работу с этим объектом другим пользователям. Допустим, что пользователь user2 является оператором, который должен вводить данные в Tab1 (например, таблицу новых заказов), а пользователь user 3 является большим начальником (например, менеджером отдела), который должен регулярно просматривать введенные данные.

Для объекта типа таблица полным допустимым перечнем действий является набор из четырех операций: SELECT, INSERT, DELETE, UPDATE. При этом операция обновления может быть ограничена несколькими столбцами.

Общий формат оператора назначения привилегий для объекта типа таблица будет иметь следующий синтаксис:

GRANT {[SELECT][.INSERT][.DELETE][,UPDATE (<списокстолбцов»)] }
ON <имятаблицы»
TO {<имяпользователя> | PUBLIC } [WITH GRANT OPTION]

Тогда резонно будет выполнить следующие назначения:

GRANT INSERT ON Tab1 TO user2 GRANT SELECT ON Tab1 TO user3

Эти назначения означают, что пользователь user2 имеет право только вводить новые строки в отношениях Tab1, а пользователь user3 имеет право просматривать все строки в таблице Tab1.

При назначении прав доступа на операцию модификации можно уточнить, значение каких столбцов может изменять пользователь. Допустим, что менеджер отдела имеет право изменять цену на предоставляемые услуги. Предположим, что цена задается в столбце COST таблицы Tab1. Тогда операция назначения привилегий пользователю user3 может измениться и выглядеть следующим образом:

GRANT SELECT. UPDATE (COST) ON Tab1 TO user3

Если наш пользователь userl предполагает, что пользователь user4 может его замещать в случае его отсутствия, то он может предоставить этому пользователю все права по работе с созданной таблицей Tab1.

GRANT ALL PRIVILEGES ON Tab1
TO user4 WITH GRANT OPTION

В этом случае пользователь user4 может сам назначать привилегии по работе с таблицей TaЫ в отсутствие владельца объекта пользователя userl. Поэтому в случае появления нового оператора пользователя user5 он может назначить ему права на ввод новых строк в таблицу командой

GRANT INSERT ON Tabl TO user5

Если при передаче полномочий набор операций над объектом ограничен, то пользователь, которому переданы эти полномочия, может передать другому пользователю только те полномочия, которые есть у него, или часть этих полномочий. Поэтому, если пользователю user4 были делегированы следующие полномочия:

GRANT SELECT, UPDATE, DELETE ON Tabl TO user4
WITH GRANT OPTION то пользователь user4 не сможет передать полномочия на ввод данных пользователю user5, потому что эта операция не входит в список разрешенных для него самого Кроме непосредственного назначения прав по работе с таблицами, эффективны'-' методом защиты данных может быть создание представлений, которые будут содержать только необходимые столбцы для работы конкретного пользователя и предоставление прав на работу с данным представлением пользователю.

Так как представления могут соответствовать итоговым запросам, то для этих представлений недопустимы операции изменения, и, следовательно, для таких представлений набор допустимых действий ограничивается операцией SELECT. Если же представления соответствуют выборке из базовой таблицы, то для такого представления допустимыми будут все 4

операции: SELECT, INSERT, UPDATE и DELETE.
Для отмены ранее назначенных привилегий в стандарте SQL определен оператор REVOKE. Оператор отмены привилегий имеет следующий синтаксис:
REVOKE {<список операций | ALL
PRIVILEGES} ON <имя объекта>
FROM {«список пользователей I PUBLIC } {CASCADE | RESTRICT }
Параметры CASCADE или RESTRICT определяют, каким образом должна производиться отмена привилегий. Параметр CASCADE отменяет привилегии не только пользователя, который непосредственно упоминался в операторе GRANT при предоставлении ему привилегий, но и всем пользователям, которым этот пользователь присвоил привилегии, воспользовавшись параметром WITH GRANT OPTION.
Например, при использовании операции:
REVOKE ALL PRIVILEGES ON Tabl
TO user4 CASCADE
будут отменены привилегии и пользователя user5, которому пользователь user4 успел присвоить привилегии.
Параметр RESTRICT ограничивает отмену привилегий только пользователю, непосредственно упомянутому в операторе REVOKE. Но при наличии делегированных привилегий этот оператор не будет выполнен. Так, например, операция:
REVOKE ALL PRIVILEGES ON Tabl
TO user4 RESTRICT не будет выполнена, потому что пользователь user4 передал часть своих полномочий пользователю user5.
Посредством оператора REVOKE можно отобрать все или только некоторые из ранее присвоенных привилегий по работе с конкретным объектом. При этом из описания синтаксиса оператора отмены привилегий видно, что

можно отобрать привилегии одним оператором сразу у нескольких пользователей или у целой группы PUBLIC.

Поэтому корректным будет следующее использование оператора REVOKE: REVOKE INSERT ON Tabl

TO user2,user4 CASCADE

При работе с другими объектами изменяется список операций, которые используются в операторах GRANT и REVOKE.

По умолчанию действие, соответствующее запуску (исполнению) хранимой процедуры, назначается всем членам группы PUBLIC.

Если вы хотите изменить это условие, то после создания хранимой процедуры необходимо записать оператор REVOKE. REVOKE EXECUTE ON COUNT EX TO PUBLIC CASCADE. Теперь мы можем назначить новые права пользователю user4:

GRANT EXECUTE

ON COUNT_EX

TO user4

Системный администратор может разрешить некоторому пользователю создавать и изменять таблицы в некоторой БД. Тогда он может записать оператор предоставления прав следующим образом:

GRANT CREATE TABLE, ALTER TABLE.

DROP TABLE ON DB_LIB TO userl

этом случае пользователь userl может создавать, изменять или удалять таблицы в БД DBLIB. Однако он не может разрешить создавать или изменять таблицы в этой БД другим пользователям, потому что ему дано разрешение без права делегирования своих возможностей.

некоторых СУБД пользователь может получить права создавать БД. Например, в MS SQL Server системный администратор может предоставить пользователю mainuser право на создание своей БД на данном сервере. Это может быть сделано следующей командой:

GRANT CREATE DATABASE ON SERVER_0 TO mainuser

По принципу иерархии пользователь mainuser, создав свою БД, теперь может предоставить права на создание или изменение любых объектов в этой БД другим пользователям.

В СУБД, которые поддерживают однобазовую архитектуру, такие разрешения недопустимы. Например, в СУБД Oracle на сервере создается только одна БД, но пользователи могут работать на уровне подсхемы (части таблиц БД и связанных с ними объектов). Поэтому там вводится понятие системных привилегий. Их очень много: 80 различных привилегий.

Для того чтобы разрешить пользователю создавать объекты внутри этой БД, используется понятие системной привилегии, которая может быть назначена одному или нескольким пользователям. Они выдаются только на действия и конкретный тип объекта. Поэтому, если вы, как системный администратор, предоставили пользователю право создания таблиц (CREATE TABLE), то для того чтобы он мог создать триггер для таблицы, ему необходимо предоставить еще одну системную привилегию CREATE TRIGGER Система защиты в Oracle считается одной из самых мощных, но это имеет и обратную сторону — она весьма сложная. Поэтому задача администрирования в Oracle требует хорошего знания как семантики принципов поддержки прав доступа, так и физической реализации этих возможностей.

Реализация системы защиты в MS SQL .ServerSQLserver 6.5 поддерживает 3 режима проверки при определении прав пользователя:

стандартный (standard);

интегрированный (integratedsecurity);

смешанный (mixed).

Стандартный режим защиты предполагает, что каждый пользователь должен иметь учетную запись как пользователь домена NT Server. Учетная запись пользователя доме- [на включает имя пользователя и его индивидуальный пароль. Пользователи доменов могут быть объединены в группы. Как пользователь домена пользователь получает доступ к определенным ресурсам домена. В качестве одного из ресурсов домена и рассматривается SQL Server. Но для доступа к SQL Server пользователь должен иметь учетную запись пользователя MS SQL Server. Эта учетная запись также должна включать уникальное имя пользователя сервера и его пароль. При подключении к операционной среде пользователь задает свое имя и пароль пользователя домена. При подключении к серверу баз данных пользователь задает свое уникальное имя пользователя SQL Server и свой , пароль.
Интегрированный режим предполагает, что для пользователя задается только одна учетная запись в операционной системе как пользователя домена, а SQL Server идентифицирует пользователя по его данным в этой учетной записи. В этом случае пользователь задает только одно свое имя и один пароль.
случае смешанного режима часть пользователей может быть подключена к серверу с использованием стандартного режима, а часть — с использованием интегрированного режима.
MS SQL Server 7.0 оставлены только 2 режима: интегрированный, называемый Windows NT Authentication Mode (Windows NT Authentication), и смешанный. Mixed Mode (Windows NT Authentication and SQL Server Authentication). Алгоритм проверки аутентификации пользователя в MS SQL Server 7.0 приведен на рис. 1.13 .

При попытке подключения к серверу БД сначала проверяется, какой метод аутентификации определен для данного пользователя. Если определен Windows NT Authentication Mode, то далее проверяется, имеет ли данный пользователь домена доступ к ресурсу SQL Server. Если он имеет доступ, то

выполняется попытка подключения с использованием имени пользователя и пароля, определенных для пользователя домена: если данный пользователь имеет права подключения к SQL Server, то подключение выполняется успешно, в противном случае, пользователь получает сообщение о том, что данному пользователю не разрешено подключение к SQL Server.

При использовании смешанного режима аутентификации средствами SQL Server проводится последовательная проверка имени пользователя (login) и его пароля (password); если эти параметры заданы корректно, то подключение завершается успешно. в противном случае, пользователь также получает сообщение о невозможности подключиться к SQL Server.

Для СУБД Oracle всегда используется в дополнение к имени пользователя и пароля в операционной среде его имя и пароль для работы с сервером БД. Второй задачей при работе с БД, как указывалось ранее, является проверка полномочий пользователей. Полномочия пользователей хранятся в специальных системных таблицах, и их проверка осуществляется ядром СУБД при выполнении каждой операции. Логически для каждого пользователя и каждого объекта в БД как бы строится некоторая условная матрица, где по одному измерению расположены объекты, а по другому— пользователи.

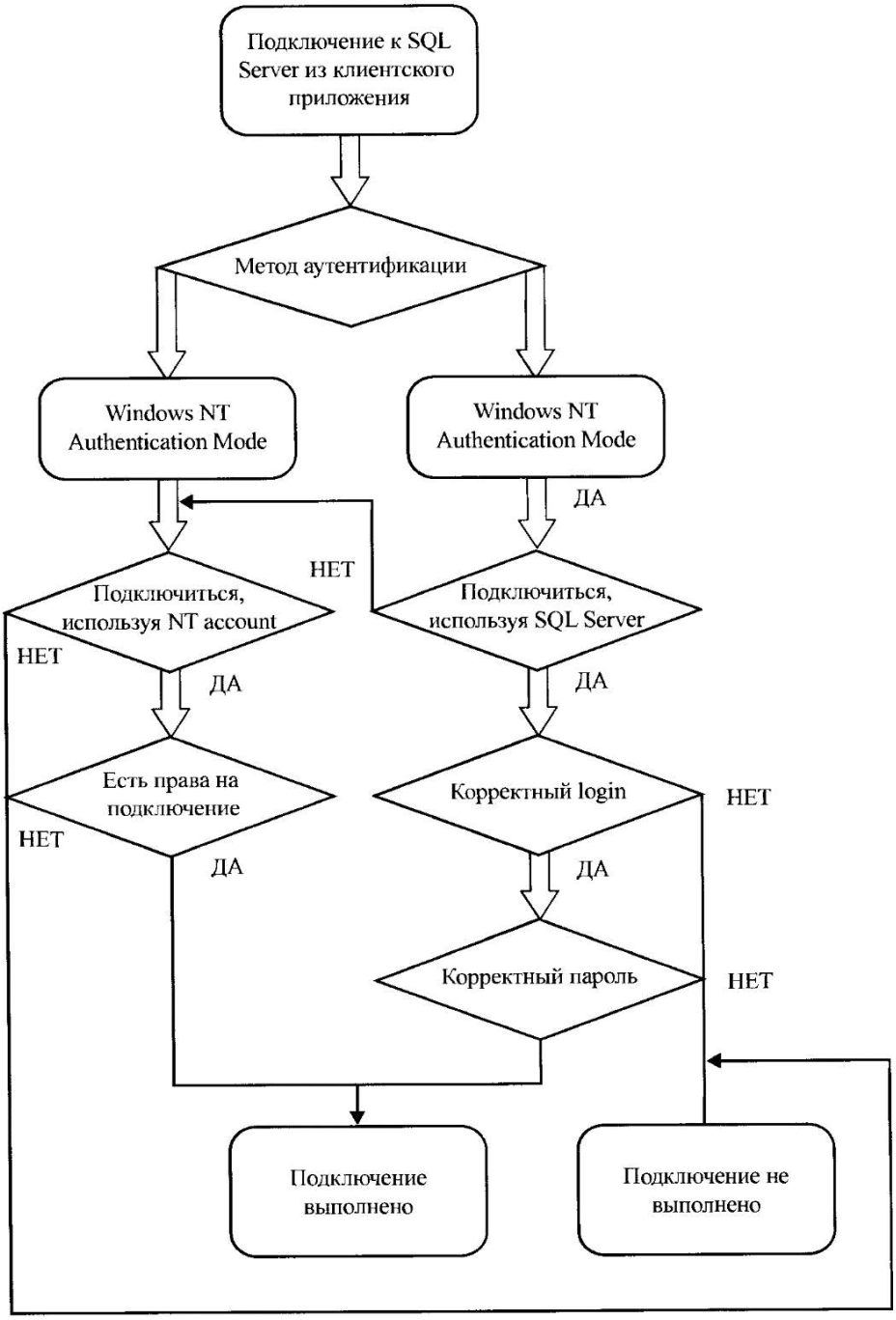


Рис. 1.13. Алгоритм проверки аутентификации пользователя в MSSQLServer

На пересечении каждого столбца и каждой строки расположен перечень разрешенных операций для данного пользователя над данным объектом. С первою взгляда кажется, что эта модель проверки достаточно устойчивая. Но

сложность тогда, когда мы используем косвенное обращение к объектам. Например, пользователю userN не разрешен доступ к таблице Tabl, но этому пользователю разрешен запуск хранимой процедуры SP N. которая делает выборку из этого объекта. По умолчанию все хранимые процедуры запускаются под именем их владельца.

Такие проблемы должны решаться организационными методами. При разрешении доступа некоторых пользователей необходимо помнить о возможности косвенного тосту па.

В любом случае проблема защиты никогда не была чисто технической задачей — это комплекс организационно-технических мероприятий, которые должны обеспечить максимальную конфиденциальность информации, хранимой в БД.

Кроме того, при работе в сети существует еще проблема проверки подлинности полномочий.

Эта проблема состоит в следующем. Допустим, процессу 1 даны полномочия по работе с БД, а процессу 2 такие полномочия не даны. Тогда напрямую процесс 2 не может обратиться к БД, но он может обратиться к процессу 1 и через него получить доступ к информации из БД.

Поэтому в безопасной среде должна присутствовать модель проверки подлинности, которая обеспечивает подтверждение заявленных пользователями или процессами идентификаторов. Проверка полномочий приобрела еще большее значение в условиях массового распространения распределенных вычислений. При существующем высоком уровне связности вычислительных систем необходимо контролировать все обращения к системе.

Проблемы проверки подлинности обычно относят к сфере безопасности коммуникаций и сетей, поэтому мы не будем их здесь более обсуждать, за исключением следующею замечания. В целостной системе компьютерной безопасности, где четкое выполнение программы защиты информации

обеспечивается за счет взаимодействия соответствующих средств в операционных системах, сетях, базах данных, проверка подлинности имеет прямое отношение к безопасности баз данных.

Заметим, что модель безопасности, основанная на базовых механизмах проверки полномочий и проверки подлинности, не решает таких проблем, как украденные пользовательские идентификаторы и пароли или злонамеренные действия некоторых пользователей, обладающих полномочиями, например, когда программист, работающий над учетной системой, имеющей полный доступ к учетной базе данных, встраивает в код программы «Троянского коня» с целью хищения или намеренного изменения информации. хранимой в БД. Такие вопросы выходят за рамки нашего обсуждения средств защиты баз данных, но следует, тем не менее, представлять себе, что программа обеспечения информационной безопасности должна охватывать не только технические области (такие, как защита сетей, баз данных и операционных систем), но и проблемы физической защиты, надежности персонале (скрытые проверки), аудит, различные процедуры поддержки безопасности, выполняемые вручную или частично автоматизированные.

Практическое задание

Разработать проект системы защиты базы данных в соответствии с закрепленным предприятием.

Контрольные вопросы

Назовите основные компоненты подсистемы защиты базы данных.

Какие наиболее общие подходы к вопросу обеспечения безопасности данных поддерживается в современных СУБД?

Перечислите наиболее известные современные СУБД.

Опишите алгоритм проверки аутентификации пользователя в MSSQLServer.
Для чего используется механизм разграничения доступа на уровне СУБД.

Лабораторная работа 15.
Изучение методов построения комплексной защиты телекоммуникационной инфраструктуры

Цель работы: изучить методы построения комплексной защиты телекоммуникационной инфраструктуры.

Теоретическая часть

Модель ISO/OSI

Особенности архитектуры компьютерных сетей описаны семиуровневой моделью взаимодействия открытых систем (Open Systems Interconnection, OSI), разработанная Международным комитетом по стандартизации ISO (чаще всего используется сокращенное наименование – «модель ISO/OSI» или просто «модель OSI»). В соответствии с концептуальными положениями этой модели процесс информационного обмена в компьютерных сетях можно разделить на семь этапов в зависимости от того, каким образом, и между какими объектами происходит информационный обмен. Эти этапы называются уровнями модели взаимодействия открытых систем. Термин «открытая система» означает, то, что при построении этой системы были использованы доступные и открыто опубликованные стандарты и спецификации. Каждому уровню модели соответствует определенная группа стандартов и спецификаций.

Далее рассмотрим последовательно особенности обработки информации на *физическом*, *канальном*, *сетевом*, *транспортном и прикладном* уровнях. По каждому уровню будут представлены сведения об уязвимостях механизмов информационного взаимодействия, характерных для данного уровня и рекомендации по устранению этих уязвимостей.

Уровень представления и *сеансовый уровень* рассматриваться не будут, так как они не содержат популярных методов защиты телекоммуникационной инфраструктуры.

Физический уровень

Самый низкий уровень модели взаимодействия открытых систем описывает процессы, происходящие на физическом уровне или уровне среды передачи. Информация, обрабатываемая в компьютерных сетях, представлена дискретными сигналами и при передаче в зависимости от характеристик среды представляется кодированием или модуляцией. Стандарты

физического уровня устанавливают требования к составляющим среды: кабельной системе, разъемам, модулям сопряжения со средой, формату сигналов при кодировании и модуляции.

Обеспечить безопасность информационного обмена на физическом уровне модели можно за счет структуризации физических связей между узлами компьютерной сети. Защищенная физическая среда передачи данных является первым рубежом для злоумышленника или преградой для воздействия разрушительных факторов окружения.

Далее приведены классификация и характеристики сред передачи, используемых при построении компьютерных сетей:

Среда передачи – *коаксиальный экранированный медный кабель*.

Использование для передачи такого типа среды предполагает наличие топологии физических связей «общая шина». Т.е. один кабельный сегмент используется для подключения всех узлов сети. Нарушение целостности кабельного сегмента приводит к отказу сети. Все узлы сети такой топологии (в том числе узел злоумышленника) имеют возможность управлять процессом передачи информации. Компьютерные сети, построенные на этом принципе, уязвимы в наибольшей степени. Злоумышленник использует механизмы разделения среды передачи в сетях этого типа для прослушивания трафика всех узлов и организации атак отказа в доступе к отдельным узлам либо всей сети в целом.

Среда передачи, образованная *медной витой парой*. Топология физических связей «звезда». Количество кабельных сегментов в данной сети соответствует количеству узлов. Нарушение целостности среды одного кабельного сегмента не влияет на работоспособность всей сети. Наиболее уязвимым элементом сети является центральное коммуникационное устройство (концентратор или коммутатор). Фактически устройства этого класса являются средством разделения среды передачи.

Концентратор образует единую среду передачи, доступную всем узлам сети. Компьютерные сети, построенные на этих устройствах, по специфике разделения физической среды передачи соответствуют сетям топологии «общая шина». Среда передачи, образованная концентратором, позволяет злоумышленнику реализовать прослушивание трафика и атаку отказа в доступе, основанную на широковещательной рассылке сообщений. При этом злоумышленник может не иметь непосредственного физического доступа к самому концентратору.

Коммутаторы используются для осуществления попеременного доступа узлов к среде передачи. Разделение физической среды передачи между узлами во времени затрудняет прослушивание сети злоумышленником и

создает дополнительную преграду для осуществления атак отказа в доступе, основанных на широковещательной рассылке сообщений в сети.

Использование тех и других устройств как средств образования среды передачи позволяет злоумышленнику вызвать отказ всей сети при наличии у него физического доступа к ним либо к системе их энергоснабжения.
Кроме того, для всех разновидностей медных кабельных систем, используемых в качестве среды передачи данных, имеет место наличие побочного электромагнитного излучения и наводок (ПЭМИН). Несмотря на свою вторичность, ПЭМИН является информативным для злоумышленника и позволяет ему анализировать пики сетевой активности, а при наличии анализатора спектра электромагнитного излучения, осуществить перехват передаваемых средой передачи сообщений.
3. Среда передачи, образованная *оптоволоконным кабелем*. Как правило, используется при построении магистральных каналов связи. Типичная топология физических связей для такого типа среды передачи – «точка-точка» и «кольцо». Однако, в последнее время, в связи с удешевлением средств коммутации, оснащенных интерфейсами для подключения оптоволокна, все чаще встречается использование этой разновидности кабеля при построении локальных сетей звездообразной топологии. Существенным преимуществом оптоволоконной кабельной системы перед медной является отсутствие ПЭМИН, что сильно затрудняет перехват передаваемых средой сообщений. Уязвимым звеном топологии «звезда» для оптоволоконной среды передачи также являются концентраторы или коммутаторы.
Важным фактором при обеспечении надежности работы компьютерной сети и, как следствие, непрерывности информационной поддержки предприятия является наличие резервных связей. Наиболее ответственные сегменты сети, используемые для связи с критически важными узлами компьютерной сети необходимо дублировать. При этом решение задачи «горячего резервирования» кабельной системы возлагается на канальный и сетевой уровни взаимодействия. Например, в случае нарушения целостности основного кабельного сегмента – коммутатор, оснащенный функцией горячего резервирования портов, осуществляет трансляцию кадров канального уровня на резервный порт. При этом подключенный к коммутатору узел, в связи с недоступностью среды передачи на основном сетевом интерфейсе начинает прием и передачу через резервный сетевой интерфейс. Использование сетевых интерфейсов узлом заранее определено приоритетами его таблицы маршрутизации.

Дополнительную защиту сети можно обеспечить за счет ограничения физического доступа злоумышленника к кабельной системе предприятия. Например, использование скрытой проводки является преградой

злоумышленнику, осуществляющему попытки мониторинга сетевой активности и перехвата сообщений с использованием средств анализа ПЭМИН.

Гибкость системы управления доступом к среде передачи данных обеспечивается за счет перспективного строительства структурированной кабельной системы (СКС) предприятия. При проектировании и строительстве СКС необходимо предусмотреть индивидуальные линии связи для всех узлов компьютерной сети. Управление конфигурацией физических связей должно осуществляться централизовано.

Ниже приведены основные рекомендации, позволяющие снизить вероятность эксплуатации кабельной системы компьютерной сети предприятия злоумышленником.

Рекомендуемая конфигурация физических связей в компьютерной сети предприятия – «звезда», при этом для подключения каждого узла выделен отдельный кабельный сегмент. В качестве среды передачи используется восьмижильный медный кабель типа «витая пара» либо оптоволокно.

Для подключения критически важных для предприятия серверов используют два кабельных сегмента – основной и резервный.

Прокладка сетевого кабеля осуществляется в скрытой проводке, либо в закрываемых кабель-каналах с возможностью опечатывания не срываемыми наклейками – «стикерами».

Кабельные сегменты, используемые для подключения всех узлов компьютерной сети, должны быть сконцентрированы на одной коммутационной панели.

В начальной конфигурации топологии физических связей должно быть исключено совместное использование среды передачи любой парой узлов сети. Исключение составляет связь с «узел-коммутатор».

Управление конфигурацией физических связей между узлами осуществляется только на коммутационной панели.

Коммутационная панель смонтирована в запираемом коммутационном шкафу. Доступ в помещение коммутационного шкафа строго ограничен и контролируется службой безопасности предприятия.

Особый класс сред передачи составляет беспроводная среда передачи или радиочастотный ресурс. При построении компьютерных сетей предприятий в настоящее время широко применяется технология RadioEthernet. Топология физических связей сетей, построенных по этому принципу, – либо «точка-точка», либо «звезда». Особенность организации беспроводных сетей передачи данных, построенных с использованием

технологии RadioEthernet, предполагает наличие у злоумышленника полного доступа к среде передачи. Злоумышленник, обладающий радиосетевым адаптером в состоянии без труда организовать прослушивание радиосети передачи данных. Парализовать работу такой сети можно при условии наличия у злоумышленника излучателя, работающего 2ГГц-овом в диапазоне частот и обладающего более высокими по сравнению с излучателями атакуемой радиосети мощностными характеристиками.
Рекомендации по защите радиосетей передачи данных.
Служба безопасности должна обеспечить строгое ограничение физического доступа персонала предприятия и полное исключение доступа посторонних на площадки монтажа приемного и излучающего оборудования радиосетей передачи данных. Доступ на площадки должен контролироваться службой безопасности предприятия.

Прокладка высокочастотного кабеля должна быть выполнена скрытым способом либо в коробах с последующим опечатыванием коробов «стикерами».

Длина высокочастотного кабельного сегмента должна быть минимальной.

Доступ в помещения с радиомодемами, радиомостами и станциями, оснащенными радиосетевыми адаптерами должен строго контролироваться службой безопасности предприятия.

Администратор сети должен детально документировать процедуры настройки радиомодемов, радиомостов и станций, оснащенных радиосетевыми адаптерами.

Администратор сети должен регулярно менять реквизиты авторизации для удаленного управления этими устройствами.
Администратор сети должен выделить отдельный адресный пул для администрирования этих устройств по сети.
Администратор сети должен отключить неиспользуемые функции радиомодемов, радиомостов и станций, оснащенных радиосетевыми адаптерами.

Администратор должен активировать функции радиомодема или радиомоста обеспечивающие «туннелирование» и криптографическую защиту передаваемых и принимаемых сообщений.

Администратор должен контролировать доступ к радиомодемам, радиомостам и станциям, оснащенным радиоадаптерами со стороны узлов компьютерной сети предприятия. Один из возможных способов контроля – использование межсетевого экрана.

Канальный уровень

Обеспечение безопасности разделения среды передачи коммуникационными средствами канального уровня. Протоколы и стандарты этого уровня описывают процедуры проверки доступности среды передачи и корректности передачи данных. Осуществление контроля доступности среды необходимо т.к. спецификации физического уровня не учитывают то, что в некоторых сетях линии связи могут разделяется между несколькими взаимодействующими узлами и физическая среда передачи может быть занята. Подавляющее большинство компьютерных сетей построено на основе технологий Ethernet, Fast Ethernet и Gigabit Ethernet. Алгоритм определения доступности среды для всех технологий одинаков и основан на постоянном прослушивании среды передачи всеми подключенными к ней узлами. Эта особенность используется злоумышленниками для организации различных видов атак на компьютерные сети. Даже при условии соблюдения рекомендаций относительно исключения разделения среды передачи злоумышленник может осуществить прослушивание трафика между произвольно выбранной парой узлов компьютерной сети. Причем использование простых коммутаторов не является серьезной преградой для злоумышленника. Утверждение о полной защищенности сетей, построенных на основе топологии физических связей «звезда» и оснащенных простыми коммутаторами, является серьезным заблуждением. Далее мы рассмотрим недостатки применения простых коммутаторов как средства обеспечения информационного обмена в компьютерных сетях на канальном уровне.

Процесс передачи информации от одного узла (А) к другому (Б) через простой коммутатор происходит поэтапно и данные передаются блоками. Размер блоков определен стандартом канального уровня. Блок данных, которым оперирует протокол канального уровня, называется кадром. Предположим, что передающий узел (А) определил доступность среды и начал передачу. В первом передаваемом кадре будет широковещательный запрос ко всем узлам сети о поиске узла с необходимым сетевым адресом. Этот запрос содержит аппаратный адрес узла отправителя (А) и его сетевой адрес (в данном случае речь идет об IP как протоколе сетевого уровня). Заметим, что коммутатор в соответствии с требованиями спецификаций канального уровня обязан передать этот широковещательный запрос всем подключенным к его портам узлам. Обратим внимание также на то, что в нашей компьютерной сети выполнено требование об исключении разделения среды передачи между двумя узлами, и каждый узел подключен

непосредственно к своему порту коммутатора. Однако, несмотря, на выполнение данной рекомендации, злоумышленник получит

широковещательный запрос узла (А), т.к. узел его (злоумышленника) может оказаться искомым. Таким образом, злоумышленник будет получать наравне со всеми остальными широковещательные запросы на разрешение сетевых адресов. Накапливая сведения из широковещательных запросов, злоумышленник будет иметь представление о сетевой активности всех узлов. Т.е. о том - кто, и в какое время и с кем пытался начать информационный обмен. С помощью этой несложной техники злоумышленник может определить аппаратные и сетевые адреса узлов являющихся серверами или маршрутизаторами. Количество запросов на разрешение сетевого адреса сервера или маршрутизатора будет на несколько порядков выше, чем обычной рабочей станции. Сформировав таким образом ведомость сетевой активности и карту сети с адресами предполагаемых серверов и маршрутизаторов, злоумышленник может сразу приступить к реализации атак отказа в доступе к этим узлам. Заметим при этом, что в процессе сбора широковещательных пакетов злоумышленник не проявлял никакой сетевой активности, т.е. оставался невидимым для всех узлов сети кроме простого коммутатора, к порту которого он подключен.

Рассмотрим, что происходит после того как узел назначения (Б) получил кадр с запросом на разрешение своего сетевого адреса. Согласно требований спецификаций канального уровня, узел, получивший широковещательный кадр, содержащий запрос на разрешение своего сетевого адреса, обязан передать отправителю этого кадра ответ, содержащий собственные сетевой и аппаратный адреса. Ответ узла (Б) будет уже не широковещательным, а адресованным узлу (А). Коммутатор, обязан транслировать ответ узла (Б) только на тот порт, к которому подключен узел (А). Таким образом, кадр канального уровня, содержащий ответ узла (Б) уже никак не попадет к злоумышленнику. Это объясняется тем, что среда передачи, используемая для подключения злоумышленника к коммутатору, будет свободна в момент передачи ответа. После получения кадра с ответом, узел (А) узнает аппаратный (MAC) адрес узла (Б) и сможет начать передачу пакетов сетевого уровня в адрес узла (Б). Дальнейшие аспекты взаимодействия узлов находятся вне компетенции протоколов канального уровня. Задача протокола канального уровня считается выполненной, если обменивающиеся данными узлы знают аппаратные адреса друг друга и могут инкапсулировать сетевые пакеты в кадры канального уровня, идентифицируемые коммутатором по MAC-адресам узлов.

Уязвимость системы разрешения сетевых адресов, описанной выше (в IP-сетях эта система называется ARP – Address Resolution Protocol) состоит в том, что узел (А) доверяет содержимому кадра с ответом. То есть данные,

переданные в ответ на запрос о разрешении сетевого адреса, никак не проверяются и ничем не подтверждаются. Этой уязвимостью и воспользуется злоумышленник, желающий подменить собой узел (Б) или прослушать поток кадров, передаваемых между любыми двумя узлами сети. Происходит это следующим образом. Злоумышленник, узел которого далее обозначим литерой (Х), заблаговременно определяет аппаратный и сетевой адреса атакуемых узлов. Затем начинает непрерывно отправлять в адрес узла (А) ложные ответы с указанием сетевого адреса узла (Б) и аппаратного адреса своего узла (Х). Получая ложные ответы узел (А) перестраивает свою таблицу разрешения сетевых адресов и с этого момента все кадры, отправляемые им в адрес узла (Б) будут иметь в заголовке аппаратный адрес узла злоумышленника. Поскольку простой коммутатор принимает решение о трансляции кадра на тот или иной порт только на основании аппаратного адреса, указанного в заголовке этого кадра, злоумышленник будет получать все сообщения, адресованные узлу (Б). Если злоумышленнику необходимо организовать прослушивание трафика между узлами (А) и (Б) он осуществляет ложную рассылку ответов в адрес обоих узлов и полученные в свой адрес кадры после просмотра и анализа транслирует узлу, которому они предназначались.

Описанная выше техника подмены аппаратных адресов (в народе известна под англоязычным названием ARP spoofing) не является новой, различные варианты ее реализации доступны пользователям сети Интернет в виде готовых программ с подробным руководством пользователя. Однако, практика показывает, что в компьютерных сетях предприятий продолжается использование дешевых простых коммутаторов на ответственных участках при подключении критически важных для предприятия узлов (серверов, маршрутизаторов и т.д.). Компьютерные сети, оснащенные многофункциональными управляемыми коммутаторами, зачастую также остаются уязвимыми к подобного рода атакам. Во многих случаях функции защиты и разграничения доступа к среде передачи, реализованные в этих изделиях, остаются невостребованными в связи с недостатком квалификации или небрежностью системных администраторов. Кроме того, эффективное разграничение доступа средствами канального уровня возможно только при условии полной инвентаризации узлов сети и формализации правил взаимодействия между ними. На практике руководство предприятия неохотно выделяет средства на проведение подобных работ, не понимая их важности для обеспечения защиты компьютерной сети.

Ниже приведены рекомендации, следование которым позволяет дополнительно защитить компьютерную сеть предприятия средствами канального уровня.
Администратор службы безопасности должен вести инвентаризационную ведомость соответствия аппаратных и сетевых адресов всех узлов сети предприятия.

Службой безопасности, совместно с отделом информационных технологий, должна быть разработана политика защиты компьютерной сети средствами канального уровня, определяющая допустимые маршруты передачи кадров канального уровня. Разработанная политика должна запрещать связи типа «один-ко-многим», не обоснованные требованиями информационной поддержки деятельности предприятия. Политикой также должны быть определены рабочие места, с которых разрешено конфигурирование средств коммутации канального уровня.
Средства коммутации канального уровня, используемые в компьютерной сети предприятия, должны быть настраиваемыми и обеспечивать разграничение доступа между узлами сети в соответствии с разработанной политикой. Как правило, такие средства поддерживают технологию VLAN, позволяющую в рамках одного коммутатора выделить группы аппаратных адресов и сформировать для них правила трансляции кадров.

Администратор сети должен выполнить настройку подсистемы управления VLAN коммутатора, и других подсистем, необходимых для реализации разработанной политики защиты. В обязанности администратора входит также отключение неиспользуемых подсистем коммутатора.
Администратор сети должен регулярно контролировать соответствие конфигураций коммутаторов разработанной политике защиты.
Администратор сети должен вести мониторинг сетевой активности пользователей с целью выявления источников аномально высокого количества широковещательных запросов.
Служба безопасности должна контролировать регулярность смены реквизитов авторизации администратора в подсистемах управления коммутаторами.

Служба безопасности должна контролировать регулярность выполнения администратором мероприятий, связанных с мониторингом сети, осуществлением профилактических работ по настройке коммутаторов, а также созданием резервных копий конфигураций коммутаторов.

9. Служба безопасности должна обеспечить строгий контроль доступа в помещения, в которых расположены коммутаторы и рабочие станции, с которых разрешено управление коммутаторами.

Сетевой уровень

Использование в компьютерной сети протоколов сетевого уровня является необходимым условием для обеспечения взаимодействия между узлами сетей с различными канальными протоколами. Сетевые протоколы позволяют преодолеть ограничения, накладываемые спецификациями канального уровня. Например, позволяют объединить компьютерную сеть предприятия с сетью интернет-провайдера с использованием телефонных сетей общего пользования. Сделать это только средствами канальных протоколов достаточно сложно. Кроме того, объединение двух различных по назначению сетей с использованием мостов крайне отрицательно сказывается на уровне защищенности объединяемых сетей. В большинстве случаев администратор и служба безопасности предприятия не могут полностью проинвентаризировать узлы подключаемой сети, и, следовательно, формализовать правила обмена кадрами канального уровня.

Второй важный аспект использования протоколов сетевого уровня – это разграничение доступа к ресурсам внутри сети предприятия, использующей только один стандарт канального уровня. Использование для этой цели протоколов сетевого уровня весьма эффективно даже для сетей, построенных с использованием только одного стандарта канального уровня. Проблема совместимости в таких сетях не актуальна, и поэтому полезные свойства сетевых протоколов можно использовать для защиты от воздействия на сеть злоумышленника. Одним из таких свойств является использование протоколами сетевого уровня раздельной схемы адресации сети (т.е. группы компьютеров) и отдельно взятого узла этой группы. В частности, адрес протокола сетевого уровня IP состоит из двух частей – номера сети, и номера узла. При этом максимально возможное количество узлов в сети или ее адресное пространство определяется значением сетевой маски или (ранее, до введения бесклассовой маршрутизации CIDR) классом сети.

Данную особенность адресации могут использовать как администратор сети, так и злоумышленник. Одной из задач администратора сети и сотрудников службы безопасности является защита адресного пространства сети от возможности его использования злоумышленником. Частично эту функцию выполняют механизмы маршрутизации, реализованные модулями протокола сетевого уровня. Т.е. осуществление обмена между узлами сетей с

различными номерами невозможно без предварительной настройки локальных таблиц маршрутизации узлов этих сетей, либо без внесения изменений в конфигурацию маршрутизатора, осуществляющего обмен пакетами (пакетом называется блок данных, с которым работает протокол сетевого уровня).

Однако почти всегда в адресном пространстве сети остается часть адресов, не занятых в настоящий момент и поэтому доступных для эксплуатации злоумышленником. Это объясняется форматом представления номера сети и номера узла IP-протокола. Количество узлов в сети – это всегда 2n, т.е. 4,8,16,32,64 и т.д. Реальное же количество узлов не бывает таким. Кроме того, администратор всегда стремится зарезервировать адресное пространство для новых узлов. Именно этот резерв может и будет использован злоумышленником для осуществления атак на функционирующие узлы компьютерной сети.

Решение проблемы очевидно – нужно использовать все адресное пространство и не дать злоумышленнику возможности захватить адреса неиспользуемых узлов. Одним из способов является применение службы мониторинга сети и поддержки виртуальных узлов в резервном диапазоне адресов. Данная служба постоянно использует свободное адресное пространство сети, создавая собственные виртуальные хосты (новые виртуальные хосты создаются сразу после отключения от сети реально функционирующих доверенных узлов). Таким образом, служба подменяет собой отсутствующие в настоящий момент рабочие станции, серверы, маршрутизаторы и т.д.

Транспортный уровень

Использование свойств транспортных протоколов создает наиболее эффективную преграду деятельности злоумышленника. Здесь для защиты используются признаки, содержащиеся в заголовках сегментов (сегмент – блок данных с которыми работает транспортный протокол) транспортного протокола. Этими признаками являются тип транспортного протокола, номер порта и флаг синхронизации соединения.

Если средствами канального уровня можно защитить аппаратуру компьютерной сети, а протоколы сетевого уровня позволяют разграничить доступ к отдельным хостам и подсетям, то транспортный протокол используется как средство коммуникации сетевых приложений, функционирующих на платформе отдельных узлов (хостов). Любое сетевое приложение использует транспортный протокол для доставки

обрабатываемых данных. Причем у каждого класса приложений имеется специфический номер транспортного порта. Это свойство может быть

использовано злоумышленником для атаки на конкретный сетевой сервис или службу, либо администратором сети для защиты сетевых сервисов и служб.

Администратор формирует политику защиты сети средствами транспортного уровня в виде ведомости соответствия хостов, используемых ими сетевых адресов и доверенных приложений, функционирующих на платформах этих хостов. Формализованная запись этой ведомости представляет собой табличную структуру, содержащую:

- перечень узлов (хостов), их символьные имена;
- соответствующие этим узлам (хостам) сетевые адреса;

перечень используемых каждым узлом (хостом) транспортных протоколов ;
перечень сетевых приложений, функционирующих в каждом узле и соответствующие этим приложениям порты транспортного протокола;
по каждому сетевому приложению необходимо установить,

является ли оно потребителем или поставщиком ресурса, т.е. разрешено ли ему инициировать исходящие соединения или принимать входящие.

Реализация политики защиты средствами транспортного уровня осуществляется с помощью межсетевых экранов (firewall). Межсетевой экран – это специализированное программное обеспечение, реализующее фильтрацию трафика в соответствии с правилами политики защиты сети средствами транспортного уровня. Как правило, данное программное обеспечение функционирует на платформе маршрутизатора, управляющего информационными потоками узлов различных сетей.

Прикладной уровень

Большинство телекоммуникационного оборудования поддерживают сетевой протокол *Secure Shell* (SSH). SSH протокол является протоколом для безопасной сети связи предназначены для относительно простой и недорогой в реализации. Первоначальная версия, SSH1, направлены на обеспечение безопасного удаленного объекта входа в систему для замены Telnet и других удаленных схем входа в систему, не представила безопасности. SSH также предоставляет более общий клиент-серверных возможностей и может быть использован для обеспечения таких сетевых функций, как передача файлов и электронной почты. Новая версия, SSH2, обеспечивает стандартизированный определение SSH и улучшает SSH1 во многих отношениях. SSH2 описана в качестве предлагаемого стандарта в документах RFC 4250 по 4256.

Для управления телекоммуникационным оборудованием рекомендуется не использовать открытый протокол *telnet*. Вместо него следует использовать шифрованный сетевой протокол *Secure Shell* (SSH).

Все запросы на доступ к ресурсам проходят через один или более списков контроля доступа ACL (Access Control List). ACL является набором правил доступа, которые задают для набора защищаемых ресурсов. Ресурсы с низким риском будут иметь менее строгие правила доступа, в то время как высококритичные ресурсы должны иметь более строгие правила доступа. ACL, по существу, определяют политику безопасности.

Доступ к сетевым ресурсам организации можно регулировать путем создания списков контроля доступа Login ACL, которые позволяют точно определить конкретные разрешения и условия для получения доступа к ресурсам внутренней сети.

Практическое задание

Разработайте проект организации защищенной телекоммуникационной инфраструктуры в соответствии с закрепленным предприятием.

Контрольные вопросы

Что называется телекоммуникационной инфраструктурой предприятия?

Назовите основные уровни модели OSI, используемые для защиты телекоммуникационной инфраструктуры.

Назовите основные компоненты защищенной телекоммуникационной инфраструктуры.

Перечислите основные методы защиты телекоммуникационной инфраструктуры на канальном уровне.

Перечислите основные методы защиты телекоммуникационной инфраструктуры на сетевом уровне.

Лабораторная работа 16.

Изучение методов построения комплексной защиты управления информационной безопасностью

Цель работы: изучить методы построения комплексной защиты управления информационной безопасностью.

Теоретическая часть

Понятие и цели управления

Социотехнические системы, представляя собой единение человека и техники, всегда характеризуются определенными целями, которые ставят перед собой люди, достигая их с помощью технических средств, с которыми общаются через интеллектуального посредника. Причем цели и допустимые стратегии социотехнической системы в реальных ситуациях принятия решений по их защите зачастую субъективны и не могут быть точно определены. Это происходит преимущественно по той причине, что, помимо объективных законов, в их функционировании существенную роль играют субъективные представления, суждения, поступки и даже эмоции людей. Действительно, при исследовании безопасности объекта информатизации, расположенного на некотором предприятии, значительное количество информации об этом объекте может быть получено от различных групп людей:

а) имеющих опыт управления предприятием и представляющих его цели и задачи, но не знающих досконально особенностей функционирования объекта информатизации;

б) знающих особенности функционирования объекта информатизации, но не имеющих полного представления о его целях;

в) знающих теорию и практику организации защиты, но не имеющих четких представлений о целях, задачах и особенностях функционирования объекта информатизации как системы в целом и т. п.

Поэтому получаемая от них информация, как правило, носит субъективный характер, а ее представление на естественном языке, не имея аналогов в языке традиционной математики, содержит большое число неопределенностей типа «много», «мало» — если речь идет о вложениях денежных средств в совершенствование системы защиты; объекта или об изменении количества персонала, работающего в подразделениях его защиты; «не выполнены частично», «выполнены частично», «почти

выполнены» и т. д. — если речь идет о выполнении требований руководящих документов по защите информации и т. д. Поэтому и описание подобной

информации на языке традиционной математики обедняет математическую модель исследуемой реальной системы и делает ее слишком грубой.
По определению С. Л. Оптнера, система — это устройство, предназначенное для решения проблем. Конечно, это определение следует относить лишь к искусственным системам (организационным, техническим, научным), которые существенно отличаются от живых. Они не обладают (да и не должны обладать) той самостоятельностью и независимостью, которая характерна для биологических объектов. Искусственные системы зависимы от субъекта и создаются под заранее спланированные цели. Состав, структура и функции таких систем подчинены достижению этих целей. Цель же создания любой искусственной системы — удовлетворение конкретной осознанной потребности человека, коллектива или общества в целом
(рис. 30).

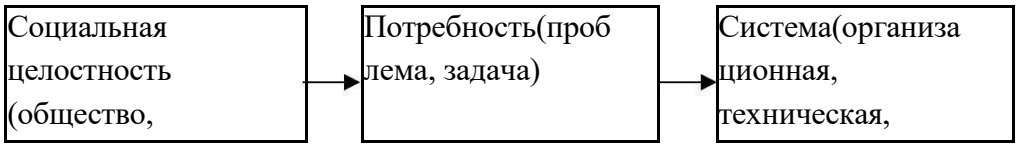


Рис. 30. Общественная потребность — основа потребления систем

Следует подчеркнуть, что общественная потребность является основой не только организационных, но и технических систем. По мнению Я. Дитриха, сущность технических систем заключается в удовлетворении человеческих потребностей в условиях общественной жизни. В процесс удовлетворения общественных потребностей входят выявление потребностей, проектирование, конструирование и эксплуатация технических средств.
связи с развитием системного анализа как основного инструментария

решении сложных проблем вместо понятия «потребность» все чаще стали использовать понятие «проблема», или «задача» («проблема» — греческое слово и в переводе означает «задача»). Связь между понятиями «проблема» и «потребность» можно выразить, определив проблему как неудовлетворенную потребность. Решить проблему — значит удовлетворить потребность, ликвидировать несоответствие между желаемым и фактическим положением дел.
Проблемы могут быть простыми и сложными. Можно различать также объектные, процессные и научно-исследовательские проблемы. Объектные проблемы выражают неудовлетворенность субъекта (общества, коллектива,

индивидуума) окружающими его объектами и требуют изменить эти объекты или создать новые. Процессные проблемы выражают неудовлетворенность

субъекта происходящими вокруг него процессами и требуют изменить эти процессы желаемым образом. Научно-исследовательские проблемы выражают неудовлетворенность субъекта своими знаниями об окружающих его объектах и наблюдаемых процессах.

Проблемы различают также:

по признаку социальной осознанности: личные, коллективные, общественные ;

до основному содержанию: экономические, социальные, политические , научные, технические;

− по возможности решения на основе целевых программ;

программируемые и непрограммируемые.

На протяжении тысячелетий люди создавали ОС, пользуясь интуицией, здравым смыслом и опытом прошлого. С возникновением письменности практический опыт построения систем стал переноситься на бумагу в виде проектов и передаваться будущему поколению. Таким образом, для построения новых ОС конструктор получил возможность пользоваться готовыми проектами аналогичных систем, хорошо зарекомендовавших себя в прошлом. Такая практика широко используется и в настоящее время. Для создания системы, имеющей аналоги в прошлом, разработчик подыскивает подходящий аналогичный проект и принимает его за основу будущей системы. Если же такого аналога; найти не удается, на помощь приходят здравый смысл и интуиция, частично дополняемые известными методами проектирования организационных структур управления, среди которых наибольшее распространение получили системный подход, нормативный метод, метод параметрическими моделирования, метод функционального моделирования и программно-целевой метод.

Разработка сложной системы разбивается на два этапа: внешнее (или макро-) и внутреннее (или микро-) проектирование. Внешнее проектирование отвечает на вопрос: с какой целью создается система?

Внутреннее — на вопрос: какими средствами реализуется система? Другими словами: «При внешнем проектировании формируется цель и критерий эффективности будущей системы, создается и экспериментально проверяется, а затем корректируется ее модель. Локализуется сама система, определяются ее границы, фиксируются факторы внешней среды, влияющие на систему или находящиеся под ее влиянием; определяются входы, на

которые система должна реагировать, и виды реакций, критерии эффективности ее функционирования. Внутреннее проектирование определяет содержание самой системы».

Этап внешнего проектирования складывается из подэтапов анализа и синтеза. На первом подэтапе формулируется цель разрабатываемой системы, проводится изучение существующей системы, составляется генеральная схема будущей системы. На втором — последовательно выполняется эскизное, техническое и рабочее проектирование системы.

КСЗИ создается с целью обеспечения надежной защиты информации на соответствующем объекте, поэтому функциями, подлежащими осуществлению в данной системе будут функции защиты, т. е. совокупность однородных отношений и мероприятий, регулярно осуществляемых на предприятии с целью создания и поддержания условий, необходимых для надежной ЗИ.

Максимально эффективной защита информации будет лишь в том случае, если созданы надежные механизмы защиты, а в процессе функционирования системы осуществляется непрерывное управление этими механизмами.

КСЗИ должно быть предусмотрено два вида функций:

− функции, основной целью которых является создание механизмов защиты ;

функции, осуществляемые с целью непрерывного и оптимального управления механизмами защиты.

Технология — это совокупность методов обработки, изменения состояния, свойств, формы сырья, материала или полуфабриката, осуществляемых в процессе производства продукции.

Исходя из вышесказанного, технологию организационного управления можно определить как регламентированную совокупность методов и средств управления коллективами людей в процессе достижения целей их деятельности .

Организационное управление прежде всего — вид человеческой деятельности и как всякая деятельность можно рассматриваться в 2 основных аспектах :

организация содержания деятельности, т. е. что делается (каковы функции и цели системы управления);

организация самого процесса, т. е. как делается (какими методами достигается поставленная цель и осуществляется сам процесс управления).

Управление определяется как элемент, функция организованных систем различной природы, обеспечивающая сохранность их определенной

структуры, поддержание режимов деятельности, реализацию их программ и целей.

Общая цель управления — обеспечение максимально возможной эффективности использования ресурсов.
Задачи управления:
Обеспечение заданного уровня достижения цели при минимальном уровне затрат;
Обеспечение максимального уровня достижения цели при заданном уровне затрат.
Технология управления должна быть построена так, чтобы обеспечивать эффективную обработку информации для всех функциональных подразделений при рациональном использовании ресурсов ВТ. При соблюдении всех правил управления и обращения с информацией это требование может быть конкретизировано следующим образом.
Технология управления должна быть разработана так, чтобы обеспечить:
комплексную автоматизацию всех процессов обработки данных и управления ;
− единство органов, средств и методов управления;

максимальную автоматизацию при решении всех задач, объективно возникающих в процессе функционирования органов управления, в том числе задач персонального информационного обеспечения, задач выработки

управленческих решений и задач информационного сопряжения взаимодействующих систем.
Одним из активных звеньев технологии управления является человек, причем человек рассматривается как субъект управления и как объект управления .
В соответствии с этим сформулируем требования к технологии управления :
Обеспечение разделения труда, выражающееся в конкретизации

функциональных обязанностей руководителей и специалистов органов управления ;
Максимальная формализация всех трудовых процессов, осуществляемых в органах управления, заключается в введении количественных оценок в управленческие процессы, в использовании математических методов в управлении, а также в применении к

управленческим системам таких понятий, как устойчивость, надежность и эффективность ;

Регламентация взаимодействия работников органов управления между собой и средствами автоматизации, которая заключается в создании комплекса правил, предписаний, указаний и ограничений, закрепленных в

соответствующих нормативно-методических документах и носящих обязательный характер;
Обеспечение психологических совместимостей руководителей и специалистов органов управления со средствами автоматизации;
Повышение исполнительской дисциплины работников органов управления.
Главным направлением построения технологии организационного управления, удовлетворяющим перечисленным выше требованиям, является разработка технологий, на индустриальной основе в широким применением вычислительной техники и автоматизации технологических процессов управления.
Чтобы разработать эффективную технологию управления, необходимо решить следующие проблемы:
Разработать, утвердить и внедрить стандартные элементы технологии управления;
Разработать и внедрить стандартные и методы решения задач всех классов;

Максимальная формализация решения всех задач, объективно возникающих в процессе функционирования системы управления;
Разработать эффективные средства, методы и способы обеспечения безопасности информации, хранимой и обрабатываемой с использованием ВТ;

Разработать нормативно-методические документы, регламентирующие взаимодействие работников органов управления между собой и со средствами автоматизации;

Разработать и внедрить типовую методологию построения и проектирования технологии организационного управления и стандартных элементов.
Таким образом, первым шагом построения технологии управления, удовлетворяющей современным требованиям, является структуризация основных процессов управления, т. е. схематизация объектов, процессов или явлений до степени однозначного определения каждого элемента.
Элемент процесса или явления считается структурированным, если он удовлетворяет следующим условиям:

Однозначность определения функционального назначения объекта, процесса или явления;
Четкость и однозначность общей архитектуры объекта процесса или явления;

Простота внутренней организации объекта, процесса или явления в целом, его составных частей и взаимосвязи между ними;

Стандартность и унифицированность внутренней структуры элементов их составляющих частей и взаимосвязей между ними;
Простота изучения структур и содержания элементов любой их совокупности и взаимосвязей между элементами;
Модульность, т. е. автономная организация элементов, позволяющая стандартными способами объединять элементы в сложные структуры, а также заменять любые элементы или совокупность этих элементов;

Гибкость, т. е. возможность расширения и реорганизации элементов

их частей без изменения или несущественными изменениями других элементов;

Доступность для изучения элементов и их частей специалистами (инперсонификация).
Структуризация основных процессов технологии управления является не только этапом разработки технологии управления, но и сама по себе позволяет в значительной степени повысить эффективность управления за счет рационализации и единой организации управления труда независимо от степени использования в управлении средств автоматизации.
Поэтому под структурированной технологией управления будем понимать управляемую совокупность приемов, правил и методов осуществления всех процессов управления.
Основные критерии построения и рационализации технологии управления:
выполнение всех процедур управления в полном объеме, своевременно и в строгом соответствии с обоснованными решениями;
максимально эффективное информационное обеспечение всего процесса управления;
максимальная автоматизация рутинных, нетворческих процедур технологии управления и информационного обеспечения.
Поэтому рационализацию технологии управления в самом общем виде можно представить последовательностью следующих действий:
Определение совокупности процедур собственно управления, подлежащих осуществлению в соответствующем интервале времени;

Определение перечня и содержания информации, необходимой для осуществления процедур управления в данном интервале времени;

3. Организация подготовки необходимой информации;

4. Организация и обеспечение осуществления процедур управления.

Структуризация процессов позволяет сама по себе независимо от использования средств автоматизации значительно повысить эффективность управления за счет лучшей ее организации. Поэтому функционирование системы управления в самом общем виде можно представить как разработку планов функционирования управляемых объектов и их реализацию.
Требования, предъявляемые к системам управления, по которым можно судить о степени организованности систем:

- детерминированность элементов;
- динамичность системы;
- наличие в системе управляющего параметра;
- наличие в системе контролирующего параметра;
- наличие в системе каналов (по крайней мере, одного) обратной связи .

Соблюдение этих требований должно обеспечивать условия эффективного уровня функционирования органов управления.

системах управления детерминированность проявляется в организации взаимодействия подразделений органов управления, при которой деятельность одного элемента (управления, отдела) сказывается на других элементах системы. Если в организационной структуре управления, например, есть отдел, действия которого не влияют на другие подразделения,

то такой отдел не реализует ни одну из целей функционирования организации и является лишним в системе управления.
Вторым требованием является динамичность, т. е. способность под воздействием внешних и внутренних возмущений оставаться некоторое время в определенном неизменном качественном состоянии.
Любые воздействия среды оказывают возмущающее действие на систему, стремясь нарушить ее. В самой системе также могут появиться возмущения, которые стремятся разрушить ее «изнутри». Например, в организации нет достаточного количества квалифицированных кадров, отсутствует по каким-то причинам ряд ответственных работников, плохие условия работы и т. д.
К внешним возмущениям следует отнести указы вышестоящих организаций, изменения ситуаций на рынке, экономические и политические факторы .
Под воздействием таких внешних и внутренних возмущений орган управления любого уровня вынужден перестраиваться, приспосабливаться к изменившимс я условиям.

С целью обеспечения быстрого перестроения системы в условиях изменения среды в системе управления должен быть элемент, фиксирующий

факт появления возмущения; система должна обладать минимально допустимой инерционностью, чтобы своевременно принимать управленческие решения, в системе управления должен быть элемент, фиксирующий факт упорядочения состояния системы в соответствии с изменившимися условиями. В соответствии с этими требованиями в структуре управления предприятием должен быть отдел совершенствования структуры управления.

Под управляющим параметром в системе управления следует понимать такой ее параметр (элемент), посредством которого можно управлять деятельностью всей системы и ее отдельными элементами. Таким параметром (элементом) в социально управляемой системе является руководитель подразделения данного уровня. Он отвечает за деятельность подчиненного ему подразделения, воспринимает управляющие сигналы руководства организации, организует их выполнение, несет ответственность за выполнение всех управленческих решений.

При этом руководитель должен обладать необходимой компетенцией, а условия работы — позволять выполнить данное поручение. Следовательно, условие наличия управляющего параметра можно считать выполненным, если, внешнюю информацию воспринимает руководитель организации, который организует работы по выполнению поручения, распределяет задания в соответствии с должностными инструкциями при наличии условий, необходимых для выполнения поручений.

Несоблюдение данного требования, т. е. наличия управляющего параметра, приводит к принятию субъективных управленческих решений и так называемому волевому стилю руководства. Это требует четкой организационной структуры и распределения обязанностей между руководителями подразделений, наличия должностных инструкций и прочих документов, регламентирующих их деятельность.

Следующим, четвертым требованием, предъявленным к системам управления, следует назвать наличие в ней контролирующего параметра, т. е. такого элемента, который постоянно контролировал бы состояние субъекта управления, не оказывая при этом на него (или на любой элемент системы) управляющего воздействия.

Контроль субъекта управления предполагает курирование обработки любого управляющего сигнала, поданного на вход данной системы. Функцию контролирующего параметра в системе управления, как правило, реализует

один из сотрудников аппарата управления. Например, подготовку плана важнейших работ курирует главный специалист по экономике. Любые

управленческие решения в системе управления должны проходить только через элемент, выполняющий функции контролирующего параметра.
Наличие прямых и обратных связей (пятое требование) в системе обеспечивается четкой регламентацией деятельности аппарата управления по приему и передаче информации при подготовке управленческих решений.
В целом структура процесса управления представлена на рис. 31 (с. 220).

Планирование деятельности

Вся сложная совокупность управленческих действий — на любом уровне и в любой системе — может быть сведена к перечню функций, составляющих замкнутый цикл управления:

− принятие управленческого решения;

− реализация решения; − контроль.

Рис. 31. Структура процесса управления

Из рис. 32 видно, что планирование является первыми шагом в цикле управления.

Планирование как функция управления имеет сложную структуру и реализуется через свои подфункции: прогнозирование, моделирование и программирование.

Прогнозирование — это метод научно обоснованного предвидения возможных направлений будущего развития организации, рассматриваемой в тесном взаимодействии с окружающей ее средой. Прогнозы носят вероятностный характер, но, если прогнозирование выполняется качественно, результатом станет прогноз будущего, который вполне можно использовать как основу для планирования.

Рис. 32. Схема связи и взаимодействия функций управления

Таким образом, прогнозирование составляет первую ступень планирования. Оно должно обеспечить решение следующих задач:

научное предвидение будущего на основе выявления тенденций и закономерностей развития;

- определение динамики экономических явлений;

определение в перспективе конечного состояния системы ее переходных состояний, а также ее поведения в различных ситуациях на пути заданному оптимальному режиму функционирования.

Важнейшее условие прогнозирования — моделирование различных ситуаций и состояний системы в течении планируемого периода.

Задача программирования — третья функция планирования, — исходя из реальных условий функционирования системы, запрограммировать ее переход в новое заданное состояние. Сюда входит разработка алгоритма функционирования системы, определение требующихся ресурсов, выбор средств и методов управления.

Таким образом, назначение планирования как функции управления состоит в стремлении заблаговременно учесть по возможности все внутренние и внешние факторы, обеспечивающие благоприятные условия для нормального функционирования и развития предприятия. Оно предусматривает

разработку комплекса мероприятий, определяющих последовательность достижения конкретных целей с учетом возможностей

наиболее эффективного использования ресурсов каждым подразделением. Поэтому планирование также должно обеспечить взаимоувязку между отдельными структурными подразделениями предприятия, включающими всю технологическую цепочку.

Обобщенные цели планирования регламентируют общий целевой подход в процессе разработки плана, а именно, выделяются две постановки целей:

а) если достижение некоторого результата является обязательным условием планируемой деятельности, то план должен разрабатываться таким образом, чтобы этот результат достигался при минимальных затратах ресурсов, т. е. нам задан результат, который должен быть достигнут при минимальном расходе ресурсов;

б) если для планируемых действий выделяются ограниченные ресурсы, то план должен быть разработан таким образом, чтобы при расходовании выделенных ресурсов достигался наибольший конечный результат, т. е. нам заданы ресурсы и при заданных ресурсах необходимо достичь максимального результата.

Планирование охватывает как текущий, так и перспективный период. Если перспективное планирование должно определять общие
стратегические цели и направления развития предприятия, необходимые для этого ресурсы и этапы решения поставленных задач, то разрабатываемые на его основе текущие планы ориентированы на фактическое достижение намеченных целей, исходя из конкретных условий. Поэтому текущие планы дополняют, развивают и корректируют перспективы направления развития с учетом конкретной обстановки.

Формы планирования в зависимости от длительности планового периода:

а) перспективное планирование (на 5 и более лет). При данном виде планирования нет ограничений по ресурсам;

б) среднесрочное планирование (от 1 до 5 лет). При данном виде планирования есть резерв ресурсов, который может быть использован;

в) текущее (рабочее) планирование (от 1 мес. до 1 года). Используют только имеющиеся ресурсы.

Отличительные особенности перспективного планирования:

− основными целями планирования является совершенствование концепции управления защиты информации; формирование планов развития средств обеспечения защиты, разработка программ оптимальных систем управления защиты проектируемых систем;

принеобходимостиможетпредусматриватьсяизменение

структурного построения функционирующих систем защиты, режимов их функционирования и технологических схем;
при необходимости могут и должны обосновываться требования к

совершенствованию концепции построения и использования системы защиты в соответствии с требованиями управления этими системами;
при разработке планов учитывают возможные условия изменения внешней среды.
Отличительные особенности среднесрочного планирования:

основные цели — рациональное использование в планируемый

период имеющихся средств и методов защиты информации, а также обоснование предложений по развитию этих средств и методов;
структура системы, как правило, изменению не подлежит, но могут

быть изменены режимы функционирования и технология управления защиты информации ;
при необходимости могут и должны разрабатываться предложения по совершенствованию структуры системы защиты, исходя из требования повышения эффективности защиты и управления системы защиты информации
.
При текущем планировании:

основной целью является рациональное использование имеющихся

средств обеспечения защиты в соответствии с планами управления комплексной системы защиты информации;
структура и режимы функционирования системы защиты

изменению не подлежат. Могут производиться лишь незначительные изменения технологии управления системы защиты информации;
при необходимости могут и должны разрабатываться предложения

по включению в состав системы управления защитой новых средств и по совершенствованию структуры этой системы.
То есть перспективное планирование предусматривает разработку общих принципов ориентации системы защиты информации на перспективу; определяет стратегическое направление и программы развития, содержание и

последовательность осуществления важнейших мероприятий, обеспечивающих достижение поставленных целей.

Поскольку оценка перспектив неопределенна, перспективное планирование не может быть ориентировано на достижение количественных показателей и поэтому обычно ограничивается разработкой лишь важнейших

качественных характеристик, конкретизируемых в программах или прогнозах.
На основе программы разрабатываются среднесрочные планы, которые уже содержат не только качественные характеристики, но и количественные показатели, детализированные и конкретизированные с точки зрения выбора средств для реализации целей, намеченных в рамках перспективного планирования.
Основными звеньями текущего плана являются календарные планы (месячные, квартальные, полугодовые), которые представляют собой детальную конкретизацию целей и задач, поставленных перспективными и среднесрочными планами.
Планирование как функция управления системой сохранения секретов реализуется через систему принципов, связанных с общими принципами управления, которые и должны быть положены в основу планирования:
директивность, т. е. обязательный характер планов;
преемственность — сочетание и взаимосвязь перспективного и текущего планирования: использование положительного опыта работы, учет допущенных недостатков и просчетов;

конкретность — постановка четких целей и задач, определение наиболее рациональных путей, методов и способов их достижения, установление ответственности конкретных лиц за организацию и выполнение плановых мероприятий, определение оптимальных и реальных сроков их реализации;
гибкость — наличие возможностей маневра имеющимися силами и средствами в ходе выполнения плана, а также корректировка плана в случае изменения обстановки;

проблемность — нацеленность мероприятий на решение значимых вопросов, сосредоточение усилий работников на основных направлениях их деятельности, недопущение распыленности в использовании сил и средств;
комплексность — обеспечение использования всей системы мер по защите тайны на различных направлениях, в подразделениях, учет интересов всех, кто ведет работу на смежных участках, согласование и увязка на различных уровнях всех задач и способов их достижения;

экономичность — максимальные результаты должны достигаться при наименьших затратах сил и средств.

Качественное планирование позволяет организовать работу по решению первостепенных, наиболее важных вопросов в конкретный период времени, добиться наилучших результатов в работе при затрате наименьших сил и средств, повысит ответственность исполнителей за порученный

участок работы, улучшит контроль, за выполнением мероприятий в установленные сроки. В процессе составления плана руководитель готовит организационную основу для объединения усилий работников в единую систему в интересах достижения поставленной цели.
Планирование может быть организовано разными способами.
Анализ. При таком способе планирования на самом высшем уровне разрабатываются основные компоненты плана: цели, задачи, возможные условия, выделенные ресурсы и др. Определяются основные задачи подразделений. Также на уровне подразделений — анализируют цели, задачи, ресурсы, сроки на уровне подразделений. Аналогично происходит на низшем уровне.

Синтез. В этом случае сначала составляют планы на низшем уровне, которые затем, последовательно обобщенные, синтезируют в соответствии и иерархической структурой.

Итерация. При таком способе определяют отправные установки планирования и на их основе вырабатывается первое приближение плана. На основе наилучшего варианта уточняются и корректируются исходные установки и разрабатывается следующее приближение плана и так до тех пор, пока не будет получен приемлемый вариант плана, который должен удовлетворять требованиям, как отдельных структур, так и всей системы в целом.
Чем выше влияние неопределенности на характер планируемой деятельности, тем более целесообразным является итерационный способ планирования. Данный способ планирования наиболее приемлем для КСЗИ.
При определении тех или иных мероприятий плана необходимо получить ответы на следующие вопросы:
Способствует ли данное мероприятие достижению поставленных задач, замыслу?
Является ли оно правомерным, не противоречит ли законам, нормативным актам?
Будет ли оно оптимальным, не дублирует ли другие мероприятия? На определение сроков осуществления намеченных мероприятий

влияют: прошлый опыт их реализации, трудоемкость, условия, в которых они будут выполняться, подготовленность исполнителей.

Содержание мероприятия должно включать: желаемый результат, краткую программу действий, планируемые к использованию, силы и средства, срок исполнения.

Основные положения вновь разработанного плана базируется на результатах проделанной работы по выполнению планов за предыдущий

период и согласовываются с планами на смежных направлениях деятельности.

В начальной стадии планирования руководитель всесторонние изучает обстановку по защите информации на предприятии, ту совокупность условий, событий, обстоятельств проведения закрытых работ, которые оказывают существенное влияние на надежность и эффективность защиты. Моделируются вероятные тенденции ее изменения, появление принципиально новых факторов (условий, событий).

Мероприятия в плане следует систематизировать по следующим четырем разделам:

организационно-методическая работа;
контрольно-проверочная работа;
профилактическая работа;
работа с кадрами.

вводной части делается анализ и оценка обстановки на предприятии с точки зрения решения вопросов по защите сведений, акцентируется внимание на ее главных особенностях. Оценка и прогноз развития обстановки служат исходной базой для определения содержания основных разделов плана.

Организационно-методическая деятельность может включать в себя:

разработку инструкций, методик по различным направлениям режима охраны информации;

внесение изменений и дополнений в действующие инструкции, методики с учетом изменившихся условий;

разработку и внедрение новых организационных методов защиты информации ;

обеспечение мероприятий в связи с приемом делегаций, командированных , участием в работе конференций и т. д.;

подготовку и проведение крупных совещаний, заседаний, экспертных комиссий, выставок и т. п.;

совершенствование системы делопроизводства, технологии обработки документов;

− сокращение закрытой переписки;

разработку и внедрение информационно-поисковых систем для классифицированных документов;
заслушивание руководителей различных уровней о ходе выполнения утвержденных директором мероприятий;
обоснование и внедрение новых технических средств охраны;

совершенствование структуры подразделения экономической безопасности , создание и оборудование новых рабочих мест;
меры по координации и взаимодействию различных подразделений предприятия и т. п.
Контрольно-проверочная работа может рассматриваться и как проверка исполнения, и как изучение состояния дел, что приближает ее к аналитической работе. Она включает в себя:
контроль за выполнением работниками предприятия требований соответствующих приказов, инструкций;
проверку выполнения мероприятий, разработанных по результатам предыдущих анализов, проверок;
контроль за порядком хранения и обращения с носителями тайны на рабочих местах;
− проверку подразделений предприятия;

проверку режима при приеме командированных лиц, делегаций, проведении совещаний;
проверку охраны, пропускного режима и т. п.
разделе профилактических мероприятий планируются действия, направленные на формирование у исполнителей мотивов поведения, побуждающих к неукоснительному соблюдению в полном объеме требований режима, правил проведения закрытых работ и т. п.
разделе работы с кадрами целесообразно включение мероприятий по обучению исполнителей и работников новым приемам, методам защиты тайны и т. п. Одним из направлений обучения и практической работы должен быть курс социально-психологических проблем взаимоотношений в коллективах лиц, допущенных к классифицированной информации.
Разработка плана невозможна без анализа предыдущей деятельности. Оцениваются имевшиеся случаи нарушения режима, причины и условия им сопутствующие. С учетом возможностей определяется надежность принимаемых мер по защите сведений. Рассматривается целесообразность привлечения необходимых средств и сил.
В процессе планирования должны быть выделены следующие стадии. 1. Обоснование целей и критериев, которое заключается в − формулировании целей, которые представляют собой совокупность
желаемых результатов и имеют иерархическую структуру. Плановые цели должны обеспечивать основу для единообразного планирования на всех

уровнях управления, предпосылки для последующего более детального планирования, основу для руководства выполнения планов, для мотивации

поведения людей, т. е. понимании ими значения выполняемых работ; основу для четкого распределения ответственности и децентрализации планирования на всех уровнях управления, для координации различной деятельности функциональных подразделений аппарата управления КСЗИ;
− выборе критериев, который определяется целями планируемой деятельности .
2. Анализ условий. На этой стадии анализируются условия, в которых будет осуществляться планируемая деятельность. Анализу подлежат как внешние условия, так и внутренние (организационная структура, характеристики персонала, имеющиеся технологические схемы и т. д.).
Кроме того, в ходе функционирования КСЗИ могут возникнуть различные непредвиденные ситуации а также система будет испытывать на себе воздействие дестабилизирующих факторов.
Все эти условия должны быть проанализированы на данной стадии. 3. Формирование задач.
Осуществляется постановка задачи и формируется комплекс задач, решение которых приведет к достижению конкретных плановых целей, а также определяются метода и разрабатываются процедуры решения каждой задачи .
4. Анализ ресурсов, которые могут быть использованы для решения задач .
Анализируют материальные (информационные, технические, программные, математические, лингвистические) и людские ресурсы. Разрабатываются прогнозы изменения этих ресурсов в процессе реализации планов .
Определение факторов, влияющих на удовлетворение потребностей в ресурсах, зависит от вида планирования, т. е. от длительности планируемого периода.
5. Согласование целей, задач, условий, ресурсов.
На этой стадии происходит выделение комплексов задач в соответствии с целями и условиями распределения ресурсов по задачам и закрепление за каждой задачей конкретных исполнителей.
6. Определение последовательности выполнения задач.
Происходит путем установления взаимосвязи результатов решений задач. Определяет время, необходимое для выполнения каждой задачи, сроки выполнения, определяются ответственные за выполнение задач.
Определение методов контроля выполнения планов:

зависит от целей планирования, выбранных критериев, а также подхода и методов планирования;

− включает в себя определение параметров плана и разработку соответствующих процедур контроля.

Методы контроля будут эффективны только тогда, когда они выявляют характер и причины отклонения от плана.

8. Определение порядка корректировки планов.

Порядок должен быть регламентирован. Корректировка должна проводиться в той мере, в какой это необходимо для достижения поставленных целей.

На этой стадии определяются параметры планов, подлежащих корректировке, условия корректировки планов, способы корректировки и разрабатываются процедуры корректировки планов.

Таким образом, можно сделать следующие основные выводы:

планирование является неотъемлемой частью деятельности КСЗИ, как и деятельности любых других систем;

от рационального планирования зависит эффективность деятельности КСЗИ, а также принятие решений в экстремальных ситуациях.

Контроль деятельности

Контроль является одним из важнейших и необходимых направлений работ по ЗИ. Цель контроля выявить слабые места системы, допущенные ошибки , своевременно исправить их и не допустить повторения.

Процесс контроля включает три стадии:

1. Установление фактического состояния СЗИ;

Анализ сравнения фактического положения с заданным режимом, обстановкой и оценка характера допущенных отклонений и недоработок;

Разработка мероприятий по улучшению и корректировке процесса управления и принятия мер по их реализации.

При принятии управленческого решения контроль выступает как источник информации, использование которого позволяет судить о содержании управленческой работы, ее качестве, результативности. Отказаться от контроля нельзя, так как это будет означать утрату информации и, следовательно, потерю управления. Контроль не является самоцелью и нужен для того, чтобы качественно обеспечить выполнение принятых решений.

Основными задачами контроля являются:

Определение обоснованности и практической целесообразности проводимых мероприятий по ЗИ;

Выявление фактического состояния СЗИ в данный период времени;

3. Установление причин и обстоятельств отклонений показателей качества, характеризующих СЗИ, от заданных;

4. Изучение деловых качеств и уровня профессиональной подготовки лиц, осуществляющих ЗИ.

Меры контроля представляют собой совокупность организационных и технических мероприятий, проводимых с целью проверки выполнения установленных требований и норм по ЗИ. Организационные меры контроля включают:

Проверку выполнения сотрудниками требований по обеспечению сохранности КТ. Такая проверка может проводиться в течение рабочего дня руководителем предприятия, его заместителем, исполнительными директорами, начальниками объектов;

Проверку выполнения пропускного режима, то есть проверка наличия постоянных пропусков у сотрудников предприятия, проверка работы охранника (на месте или нет, проверяет пропуска или нет). Может проводиться ежедневно начальником охраны объекта;

Проверку выполнения сотрудниками правил работы с конфиденциальными документами (правила хранения, размножения и копирования) проводится заместителем руководителя в любое время;

Проверку наличия защищаемых носителей конфиденциальной информации проводят сотрудники предприятия в конце рабочего дня.

При этом могут применяться следующие виды контроля:

− предварительный;

− текущий; − заключительный.

Предварительный контроль обычно реализуется в форме определенной политики, процедур и правил. Прежде всего, он применяется по отношению к трудовым, материальным и финансовым ресурсам. Предварительный контроль осуществляется при любых изменениях состава, структуры и алгоритма функционирования СЗИ, т. е. при установке нового технического устройства, при приеме нового сотрудника, при проведении ремонтных работ.

Текущий контроль осуществляется, когда работа уже идет и обычно производится в виде контроля работы подчиненного его непосредственным начальником.

Заключительный контроль осуществляется после того, как работа закончена или истекло отведенное для нее время.

Также с целью обеспечения систематического наблюдения за уровнем защиты может осуществляться периодический контроль. Периодический контроль (ежедневный) проводится сотрудниками предприятия в части

проверки наличия носителей информации, с которыми они работают. Периодический контроль может быть гласным и негласным.

Гласный периодический контроль эффективности ЗИ проводится выборочно (применительно к отдельным структурным подразделениям или отдельным работам) или на всем предприятии по планам, утвержденным руководством.

Негласный контроль осуществляется с целью объективной оценки уровня ЗИ и, прежде всего, выявления слабых мест в СЗИ. Кроме того, такой контроль оказывает психологическое воздействие на сотрудников, вынуждая их более тщательно выполнять требования по обеспечению ЗИ. Добросовестное и постоянное выполнение сотрудниками требований по ЗИ основывается на рациональном сочетании способов побуждения и принуждения. Принуждение — способ, при котором сотрудники вынуждены соблюдать правила обращения с носителями конфиденциальной информации под угрозой материальной, административной или уголовной ответственности. Побуждение предусматривает использование для создания у сотрудников установки на осознанное выполнение требований по ЗИ моральных, этических, психологических и других нравственных мотивов. Поэтому на эффективность защиты влияет климат на предприятии, который формируется его руководством.

Практическое задание

Разработайте проект организации защиты управления информационной безопасностью инфраструктуры в соответствии с закрепленным предприятием.

Контрольные вопросы

Что называется системой управления информационной безопасностью?

Какие стадии включает в себя процесс контроля целостности системы защиты информации?

Назовите основные компоненты системы управления информационной безопасностью.

Перечислите основные методы защиты систем управления информационной безопасностью.

Лабораторная работа 17.
Изучение методики составления испытаний системы защиты информации

Цель работы: научиться составлять комплексную методику испытаний системы защиты, для выявления недоработок спроектированной системы защиты.

Теоретическая часть

В соответствии с «Доктриной информационной безопасности Российской Федерации» обеспечение безопасности информационных ресурсов от несанкционированного доступа представляет собой одну из составляющих национальных интересов России в информационной сфере. Это определяет необходимость выполнения специальных действий по оценке соответствия средств защиты информации от несанкционированного доступа, используемых при построении автоматизированных систем (АС), требованиям нормативных и иных документов по защите информации. В данной статье рассматриваются инструментальные средства и методы, которые могут быть использованы при проведении функционального тестирования систем и комплексов защиты по требованиям безопасности информации в соответствии с требованиями руководящих документов.

Испытания средств защиты информации от несанкционированного доступа

Как известно, руководящий документ (РД) «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) устанавливает 7 классов защищенности средств защиты информации (СЗИ) от несанкционированного доступа (НСД) на базе перечня показателей защищенности и совокупности описывающих их требований. Рассмотрим общий порядок проведения испытаний СЗИ от НСД на соответствие требованиям РД, предъявляемым к дискреционному принципу контроля доступа, а также к механизму очистки внешней памяти.

Порядок проведения данной проверки в общем случае выглядит следующим образом (рис. 1).

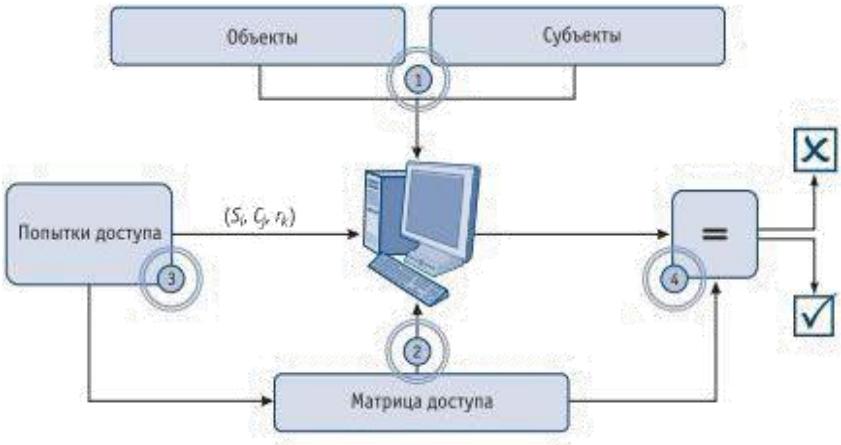


Рисунок 1 - Порядок проведения проверки

Порядок проведения данной проверки в общем случае выглядит следующим образом (рис. 1).

1) Создание тестовых субъектов(например, пользователей) S = {S1, S2, ..., Si, ..., Sn} и объектов доступа (например, объектов файловой системы) O = {O1, O2, ..., O, ..., On}.

Настройка правил разграничения доступа субъектов испытываемого СЗИ от НСД к тестовым защищаемым объектам. Данная операция заключается в настройке матрицы доступа. Строка матрицы доступа соответствует субъекту Si, а столбец – объекту Oj. На пересечении строки и столбца указаны права доступа rv.Соответствующего субъекта к данному объекту.

Тестирование фактического наличия права rky субъекта Sjпо отношению к объекту Oj(тестирование настроек СЗИ от НСД).

Сравнение фактических правдоступа с требуемыми правами, определенными в матрице доступа.

Для автоматизации процесса проверки реализации данного требования РД могут быть использованы программы семейств «Ревизор», «НКВД» или программы, написанные на языках сценариев (например, Perl или Python).

Порядок проведения данной проверки в общем случае выглядит следующим образом:

Настройка механизма очистки внешней памяти тестируемого СЗИ от НСД в соответствии с информацией, приведенной в эксплуатационной документации.

Создание тестовой последовательности символов на внешнем накопителе ЭВМ, на которой установлено тестируемое СЗИ от НСД.

Определение сектора накопителя, в котором располагается тестовая последовательность символов: данный сектор определяется путем поиска

тестовой последовательности на накопителе с использованием специализированного программного обеспечения (ПО).
Удаление созданного действием 2 файла путем применения штатных средств гарантированного удаления информации СЗИ от НСД.
Выполнение анализа сектора внешнего накопителя, определенного действием 3, на предмет наличия в нем созданной ранее последовательности символов (выполняется с помощью специализированного программного обеспечения).
Если тестовая последовательность не обнаружена, эксперт испытательной лаборатории (ИЛ) выносит вердикт о соответствии тестируемого СЗИ от НСД требованию РД[1] к очистке внешней памяти.
При проведении проверки реализации данного требования РД [1] могут быть использованы программный комплекс «Средство анализа защищенности «Сканер-ВС» (ПК «Сканер-ВС»), программы семейств
Terrier, «НКВД».
Требования к СЗИ от НСД, обеспечивающим безопасное взаимодействие сетей ЭВМ посредством управления межсетевыми потоками информации, предъявляет РД [2] «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997). Наиболее трудоемкие требования с точки зрения процесса поведения сертификационных испытаний предъявляются к функциям управления доступом (фильтрация данных и трансляция адресов).
Порядок проведения данных проверок в общем случае выглядит следующим образом (рис. 2).

Рисунок 2 - Порядок тестирования функций МЭ 1) Настройка правил фильтрации МЭ в соответствии с проверяемым
требованием РД [2].

Запуск ПО перехвата и анализа сетевых пакетов во внутреннем и внешнем сегментах сети.

Генерация сетевых пакетов из внутренней сети во внешнюю (или наоборот), прохождение которых разрешается (запрещается) в соответствии с правилами фильтрации межсетевого экрана.

Завершение перехвата сетевых пакетов, экспорт журнала регистрации разрешенных и запрещенных пакетов МЭ.
Исходя из полученных данных, эксперт ИЛ делает вывод о соответствии или несоответствии фактических (пакеты на входном интерфейсе МЭ, пакеты на выходном интерфейсе МЭ и фрагмент журнала регистрации событий МЭ) и ожидаемых результатов (правила фильтрации МЭ) тестирования. При их соответствии выносится вердикт о том, что МЭ отвечает требованию РД.
При проведении тестирования реализации требования РД к функциям управления доступом могут быть использованы, например, следующие программы: nmap, Packet Generator (генерация сетевых пакетов), wireshark, tcpdump (перехват и анализ сетевых пакетов), ПК «Сканер-ВС» (генерация сетевых пакетов, перехват и анализ сетевых пакетов).
Обязательный анализ защищенности АС выполняется в форме аттестации или сертификации на соответствие руководящего документа Гостехкомисии .
В ходе проведения проверки анализируются фактические настройки СЗИ АС, их соответствие требованиям нормативных документов и эксплуатационной документации АС. Основное отличие от процедуры испытаний СЗИ заключается в том, что проверяемая АС должна быть настроена в соответствии с требованиями нормативных документов до начала проведения испытаний. Задача эксперта ИЛ(или органа по аттестации) заключается в анализе текущих настроек СЗИ АС и их влияния на безопасность информации, обрабатываемой в АС.При проведении анализа защищенности могут применяться программные продукты, используемые для проведения испытаний СЗИ по требованиям безопасности информации. Более подробную информацию о методах и инструментальных средствах, используемых при проведении анализа защищенности АС, можно найти в работе.
В качестве инструментального комплекса испытаний удобно воспользоваться средством анализа защищенности «Сканер-ВС»,позволяющим проводить

большое количество типов проверок в соответствии с требованиями руководящих документов. Варианты использования программного комплекса (ПК) «Сканер-ВС» при проведении

функционального тестирования систем и комплексов защиты по требованиям безопасности информации приведены далее по тексту.

1. РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992):

− генерация сетевых пакетов с необходимым для проведения испытаний набором атрибутов;

− перехват и анализ сетевых пакетов.

2. РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации (Гостехкомиссия России, 1997):

− проверка механизма очисткивнешней памяти.

3. РД «Автоматизированные системы. Защита от несанкционированного доступа к информации.

Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992):

− проверка очистки освобождаемых областей внешней памяти;

− проверка подсистемы межсетевого экранирования;

− поиск уязвимостей в ресурсахсети; − локальный аудит паролей учетных записей ОС.

ПК «Сканер-ВС» обладает рядом заметных достоинств:

Полнота инструментария. ПО, входящее в состав ПК «СканерВС», позволяет проводить широкий диапазон проверок систем и комплексов защиты по требованиям РД ФСТЭК России и приказов Министра обороны Российской Федерации.

Простота использования. ПК «Сканер-ВС» представляет собой носитель информации, который запускает свою собственную среду (операционная система, производная от Linux) с предустановленным тестовым ПО. Это позволяет сократить временные расходы экспертов ИЛ на поиск, установку и настройку ПО, применяемого при проведении испытаний, в том числе и операционной системы, под которой функционирует тестовое ПО.

Сертификаты соответствия. ПК «Сканер-ВС» является сертифицированным в системах сертификации СЗИ ФСТЭК России Минобороны России средством контроля эффективности применения СЗИ.

Практическое задание

В соответствии с рассмотренными методиками разработайте план мероприятий по испытанию системы защиты объекта информатизации.

Контрольные вопросы

Назовите порядок проведения испытаний системы защиты.

Назовите порядок разработки методики испытаний.

Какой нормативный документ устанавливает 7 классов защищенности средств защиты информации?

Назовите порядок тестирования функций МЭ.

Каким рядом заметных достоинств обладает программный комплекс «Сканер-ВС»?

Учебно-методическая литература

Методические указания к практическим занятиям по дисциплине "Технология построения защищенных автоматизированных систем" для студентов специальности 090105 Комплексное обеспечение информационной безопасности автоматизированных систем / сост. Граков В. И. ; рец. Чипига А. Ф. - Ставрополь : СевКавГТУ, 2006. - 30 с. - Библиогр.: с. 29(4 назв.)

Чипига, А. Ф. (СевКавГТУ). Многоканальные измерительные системы для мониторинга безопасности объектов : учеб. пособие / А. Ф. Чипига, В. В. Федоренко, И. В. Федоренко ; ФБГОУ Сев.-Кав. гос. техн. ун-т. - Ставрополь : Издательство СевКавГТУ, 2011. - 126 с. : ил. - Библиогр.: с. 123-128 (58 назв.)

Чипига, А. Ф. Информационная безопасность автоматизированных систем : учеб. пособие / А. Ф. Чипига. – М. : Гелиос АРВ, 2010. – 336 с.

Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. – 3-е изд., стер. – Москва : Академия, 2008. – 331 с.

Чипига, А. Ф. (СевКавГТУ). Информационная безопасность : учеб. пособие (практикум) / А. Ф. Чипига, М. А. Лапина, В. В. Белоус ; М-во образования и науки Рос. Федерации, ГОУ ВПО Сев.-Кав. гос. техн. ун-т. – Ставрополь : СевКавГТУ,
2009. – 282 с.

Сергеева Ю. С. Защита информации. Конспект лекций. Учебное пособие. - М.: А-
Приор, 2011. - 128 с.

Сычев Ю. Н., Основы информационной безопасности. Учебно-практическое пособие - М.: Евразийский открытый институт, 2010.
- 328 с.

Шаньгин В. Ф., Защита компьютерной информации. Эффективные методы и средства - М.: ДМК Пресс, 2010. - 544 с. Допущено УМО вузов по университетскому политехническому образованию в качестве учебного пособия для студентов высших учебных заведений.

Аверченков В. И. , Рытов М. Ю. , Кувыклин А. В. , Гайнулин Т. Р. Методы и средства инженерно-технической защиты информации : учебное пособие. 2-е изд.,
стер. - М.: Флинта, 2011. - 187 с.

Аверченков В. И. , Рытов М. Ю. , Кувыклин А. В. , Гайнулин Т. Р. Разработка системы технической защиты информации: учебное пособие. 2-е изд., стер. -
М.: Флинта, 2011. - 187 с.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания к самостоятельным работам Комплексное обеспечение информационной безопасности автоматизированных систем

Содержание дисциплины

Основные вопросы разделов и тем

Постановка проблемы комплексного обеспечения информационной безопасности автоматизированных систем.

Системный подход к защите информации. Основные цели и задачи систем защиты
информации. Цели защиты информации. Основные задачи систем защиты информации.

Состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ), функциональные и обеспечивающие подсистемы, технология,
управление.

Управление проектами. Сетевое планирование. Управление стоимостью. Управление проектными рисками. Планирование систем для бизнеса. Системное (тотальное) управление качеством.

Методология формирования задач защиты.

Методология формирования задач защиты информации. Интеграция средств информационной безопасности в технологическую среду.

4. Интеграция средств информационной безопасности в технологическую среду.

Принципы проектирования систем защиты информации. Основные средства систем защиты информации. Стратегии применения средств защиты информации. Порядок и особенности проведения испытаний КСИБ. Порядок и особенности внедрения КСИБ в эксплуатацию.

Этапы проектирования КСИБ и требования к ним.

Предпроектное обследование; техническое задание; техническое проектирование; рабочее проектирование; испытания и внедрение в эксплуатацию; сопровождение**.**

6. Особенности проектирования на современном уровне и синтез КСИБ.

Многокритериальный синтез. Критериальный язык описания выбора. Учет при синтезе различного вклада функциональных подсистем в эффективность целостной системы. Синтез систем на основе качественных классификационных признаков. Метод морфологического древовидного синтеза. Морфологический метод лабиринтного синтеза.

Типовая структура комплексной системы защиты информации от несанкционированного доступа (НСД).
Методика выявления возможных каналов НСД; последовательность работ при
проектировании комплексной системы защиты информации от НСД и утечки за счет ПЭМИН; моделирование как инструментарий проектирования; методика построения административного управления КСИБ.

Мониторинг и контроль состояния окружающей среды.
Общие сведения о поисковых мероприятиях. Перечень поисковых работ.

Ведение специальной информационной базы данных КСИБ.
Методы и методики проектирования.
Методы нормативного функционального наполнения; метод экспертных структурных вопросников; метод оценки уязвимости информации Хоффмана; метод оценки риска ФишерА.

Методы и методики оценки качества КСИБ.
Общие сведения об оценке качества КСИБ. Методы оценки качества КСИБ. Метод экспертных оценок. Оценка качества КСИБ методом экспертных структурных вопросников. Общая характеристика метода. Этапы экспертного оценивания. Морфологический анализ. Оценка качества КСИБ методом оценки уязвимости информации Хоффмана. Оценка уязвимостей по Дж. Хоффману. Оценка качества КСИБ методом оценки риска Фишера. Оценка рисков по двум факторам. Оценка рисков по трем факторам.

Требования к эксплуатационной документации КСИБ, аттестация по требованиям
безопасности.
Комплект документов, поставляемых предприятием-изготовителем. Формуляр (технический паспорт, паспорт). Техническое описание. Инструкция по эксплуатации. Документация, разрабатываемая на месте эксплуатации. Паспорт-формуляр. Положение по обеспечению

информационной безопасности предприятия (организации). Другие документы.

Особенности эксплуатации КСИБ на объекте защиты, организационно-функциональные задачи службы безопасности.
Основы, направления и этапы защиты информации. Правовые аспекты защиты информации . Общие сведения. Подсистема организационно-правовой защиты. Промышленный шпионаж и законодательство. Защита программного обеспечения авторским правом. Стандарты и рекомендации по защите информации. Недостатки существующих стандартов и рекомендаций. Требования к содержанию нормативно-методических документов по ЗИ. Разработка нормативно-методической основы ЗИ.

Перечень примерных контрольных вопросов и заданий для самостоятельной работы по темам (модулям).
Организационно-штатная структура службы безопасности.
Функциональные задачи службы защиты информации.
Основы, направления и этапы защиты информации.
Правовые аспекты защиты информации .
Аттестация объектов по требованиям информационной безопасности.
Положение по обеспечению информационной безопасности предприятия (организации).
Методика построения административного управления КСИБ.
Порядок и особенности проведения испытаний и внедрения в эксплуатацию КСИБ.

Постановка проблемы комплексного обеспечения информационной безопасности автоматизированных систем.

Темы курсовых работ, рефератов.
Не предусмотрены

Примерный перечень вопросов к зачету (экзамену) по модулям учебной дисциплины.
Вопросы для подготовки к зачету

Организационное обеспечение информационной безопасности как составная часть системы комплексного противодействия информационным угрозам.

Структура и задачи органов власти и управления, отвечающих за организацию защиты информации в стране.
Основные принципы построения организационного обеспечения защиты информации и предъявляемые к ней требования.
Основные цели и задачи организационного обеспечения информационной безопасности на предприятии.
Объекты и субъекты организационного обеспечения защиты информации коммуникативного процесса.
Угрозы информационной безопасности. Виды угроз. Организационные меры противодействия различным видам угроз.
Случайные и преднамеренные угрозы. Меры организационного противодействия случайным и преднамеренным угрозам.
Утечка информации. Каналы утечки информации. Разглашение информации. Несанкционированный доступ. А.Н.В.
Классификация каналов утечки информации относительно возможных действий нарушителя информационной безопасности.
Содержание аналитических документов, необходимых для разработки «Политики информационной безопасности предприятия».

Структура и содержание документа «Политика информационной безопасности предприятия».
Служба информационной безопасности предприятия. Состав, цели и задачи службы информационной безопасности предприятия.
Концепция информационной безопасности предприятия. Цели и задачи предприятия в обеспечении информационной безопасности при взаимодействии с внешними и внутренними субъектами информационного обмена.

Роль стандартов и требований по информационной безопасности предприятия в формировании «Политики информационной безопасности предприятия». Принципы распределения полномочий.

Процедуры и методы информационной безопасности предприятия как составляющие «Политики информационной безопасности предприятия». Профили защиты.

Права и обязанности руководящего состава и сотрудников службы информационной безопасности. Роль служебных комиссий и «кризисных групп» в обеспечении информационной безопасности.

Порядок установления режима конфиденциальности информации. Перечень сведений, относимых к конфиденциальной информации и не подлежащих засекречиванию.
Организация конфиденциального делопроизводства.

Общие обязанности сотрудников по неразглашению конфиденциальной информации. Закрепление основных обязанностей в трудовом договоре.
Организация доступа и допуска сотрудников к конфиденциальной информации.

Порядок допуска предприятий к работам по созданию средств защиты конфиденциальной информации и к работам по оказанию услуг в области защиты конфиденциальной информации.

Организация доступа к информационным системам, обрабатывающим конфиденциальную информацию. Матричный и мандатный подходы к проблемам разграничения доступа.
Порядок обеспечения сохранности конфиденциальной информации при постоянном или временном прекращении пользователем доступа к конфиденциальному информационному ресурсу.

Возможные причины утечки информации при нарушении персоналом правил работы с конфиденциальной информацией.
Требования, предъявляемые к претендентам на работу с конфиденциальной информацией и к претендентам на должность службу информационной безопасности.
Кадровая политика предприятия. Возможные источники пополнения предприятия кадрами для работы с конфиденциальной информацией.
Порядок организации и проведения конкурсов на замещения вакантных должностей, связанных с безопасностью информации.

Методы проверки кандидатов на работу. Отражение вопросов информационной безопасности в трудовых и коллективных договорах.
Текущая работа с персоналом, допущенным к конфиденциальной информации. Дисциплинарная ответственность. Меры поощрения и наказания.

Методы борьбы с нарушениями информационной безопасности. Порядок завершения текущей работы с сотрудниками, владеющими конфиденциальной информацией при их увольнении.

Организация служебного расследования по фактам утечки конфиденциальной информации. Порядок проведения служебного расследования по фактам утраты секретных документов и разглашения конфиденциальной информации.

Сложные инциденты. Порядок организации служебного расследования в случаях возникновения сложных инцидентов.
Организация охраны объектов информатизации. Составные элементы системы охраны. Требования к охранникам и их обязанностям.
Организация режима охраны объекта. Принципы охраны. Факторы, влияющие на выбор приѐмов и средств охраны.
Организация внутриобъектового и пропускного режимов на объектах информатизации. Цели организации внутриобъктового режима.
Зона режимности предприятия. Требования к введению внутриобъктового режима.
Организация пропускного режима. Типы пропусков. Учѐт пропускных документов.

Атрибутивный и биометрический способы идентификации сотрудников. Их преимущества и недостатки.
Порядок соблюдения объектового режима при работе с представителями сторонних организаций.
Возможные каналы утечки информации из помещений, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия. Требования СТР-К по защите помещений. Организация борьбы с утечкой информации из помещений.

Аттестация помещений, в которых обрабатывается конфиденциальная информация. Этапы проведения аттестации. Технический паспорт на помещение и аттестат соответствия.

Порядок организации работ по созданию и эксплуатации объектов информатизации и средств защиты информации (СЗИ), определяемый СТР-К. Стадии создания объекты информации.

Порядок организации эксплуатации автоматизированных систем и их средств защиты информации. Особенности защиты информации при использовании съемных накопителей информации большой емкости для АРМ на базе автономных ЭВМ.

Порядок защиты информации в СУБД. Защита информации в локальных вычислительных сетях и при выходе в сети общего пользования.
Организация защиты информации при взаимодействии со сторонниками организациями. Порядок отбора и подготовки информации к оглашению. Отражение вопросов защиты информации при подготовке договоров.

Обеспечение защиты информации при ведении переговоров и при приеме в организации сторонних организаций и посетителей. Особенности обеспечения безопасности информации при приеме иностранных делегаций.

Роль информационно-аналитичной работы как составной части организационных методов защиты информации. Основные показатели качества информации. Методы прогнозирования и верификации.

Контроль функционирования системы организационной защиты информации. Формы контроля.
Аудит информационной безопасности. Формы аудита. Особенности аудита автоматизированных информационных систем.
Организационные меры по обеспечению и поддержанию информационной безопасности в период чрезвычайных ситуаций. Требования пожарной безопасности к объектам информатизации. Вопросы для подготовки к экзамену

Вопросы для подготовки к экзамену
Понятие и сущность КСЗИ.

Назначение КСЗИ.
Задачи КСЗИ.
КСЗИ как средство выражения концептуальных основ защиты информации.
Методология защиты информации как теоретический базис построения КСЗИ.
Методологические основы организации КСЗИ.
КСЗИ как сложная человеко-машинная система.
Основные положения теории систем.
Принципы организации КСЗИ.

Основные требования, предъявляемые к КСЗИ. Содержательная характеристика этапов разработки КСЗИ.
Основные факторы, влияющие на организацию КСЗИ:
организационно-правовая форма и характер основной деятельности предприятия;
состав, объем и степень конфиденциальности защищаемой информации;
структура и территориальное расположение предприятия;
режим функционирования предприятия;
конструктивные особенности предприятия;
количественные и качественные параметры ресурсообеспечения;
степень автоматизации основных процедур обработки защищаемой информации.
Характер и степень влияния различных факторов на организацию КСЗИ.
Методика определения состава защищаемой информации.
Этапы работы по выявлению состава защищаемой информации.

Функции руководства предприятия и подразделений предприятия, экспертной комиссии, службы защиты информации.
Классификация информации по видам тайны и степеням конфиденциальности.
Нормативное закрепление состава защищаемой информации;
структура перечней сведений, относимых к различным видам тайны.
Порядок внедрения перечней, внесения в них изменений и дополнений.
Значение носителей защищаемой информации как объектов защиты.
Факторы, определяющие состав носителей информации.
Методика выявления состава носителей защищаемой информации.
Хранилища носителей информации как объект защиты.
Особенности помещений для работы с защищаемой информацией как объектов защиты.

Состав технических средств обработки, передачи, транспортировки и защиты информации, являющихся объектами защиты.
Состав средств обеспечения функционирования предприятия, подлежащих защите.
Факторы, определяющие необходимость защиты периметра и здания предприятия.
Специфика персонала предприятия как объекта защиты.

Определение источников дестабилизирующего воздействия на информацию и видов их воздействия.
Методика выявления способов воздействия на информацию.

Определение причин, обстоятельств и условий дестабилизирующего воздействия на информацию.
Оценка ущерба от потенциального дестабилизирующего воздействия на информацию.
Методика выявления каналов несанкционированного доступа к информации.

Соотношение между каналами несанкционированного доступа и источниками воздействия на информацию.

Определение возможных методов несанкционированного доступа к защищаемой информации.
Оценка степени опасности применения различных методов. Анализ потенциальных последствий реализации несанкционированного доступа.
Методика выявления нарушителей (незаконных пользователей) и состава интересующей их информации.
Определение направлений и возможностей доступа нарушителей к защищаемой информации.

Оценка степени уязвимости информации в результате действий нарушителей различных категорий.

БИЛЕТ № 1
Понятие и сущность КСЗИ. Назначение КСЗИ.

Методика выявления нарушителей (незаконных пользователей) и состава интересующей их информации.

БИЛЕТ № 2

Задачи КСЗИ. КСЗИ как средство выражения концептуальных основ защиты информации.

Определение направлений и возможностей доступа нарушителей к защищаемой информации.

БИЛЕТ № 3 1. Методология защиты информации как теоретический базис построения КСЗИ.

2. Оценка степени уязвимости информации в результате действий нарушителей различных категорий.

БИЛЕТ № 4

Методологические основы организации КСЗИ. КСЗИ как сложная человеко-машинная система.

Методика выявления каналов несанкционированного доступа к информации.

БИЛЕТ № 5

Основные положения теории систем. Принципы организации КСЗИ.

Соотношение между каналами несанкционированного доступа и источниками воздействия на информацию.

БИЛЕТ № 6

Основные требования, предъявляемые к КСЗИ.

Определение возможных методов несанкционированного доступа к защищаемой информации.

БИЛЕТ № 7

Содержательная характеристика этапов разработки КСЗИ.

Анализ потенциальных последствий реализации несанкционированного доступа.

БИЛЕТ № 8

Основные факторы, влияющие на организацию КСЗИ. Организационно-правовая форма и характер основной деятельности предприятия.

Определение источников дестабилизирующего воздействия на информацию и видов их воздействия.

БИЛЕТ № 9

Основные факторы, влияющие на организацию КСЗИ. Состав, объем и степень конфиденциальности защищаемой информации.

Методика выявления способов воздействия на информацию

БИЛЕТ № 10

Основные факторы, влияющие на организацию КСЗИ. Структура и территориальное расположение предприятия.

Определение причин, обстоятельств и условий дестабилизирующего воздействия на информацию.

БИЛЕТ № 11

Основные факторы, влияющие на организацию КСЗИ. Степень автоматизации основных процедур обработки защищаемой информации.

Оценка ущерба от потенциального дестабилизирующего воздействия на информацию.

БИЛЕТ № 12

Методика определения состава защищаемой информации.

Значение носителей защищаемой информации как объектов защиты. Факторы, определяющие состав носителей информации.

БИЛЕТ № 13 1. Этапы работы по выявлению состава защищаемой информации.

2. Методика выявления состава носителей защищаемой информации. Хранилища носителей информации как объект защиты.

БИЛЕТ № 14

Классификация информации по видам тайны и степеням конфиденциальности.

Особенности помещений для работы с защищаемой информацией как объектов защиты.

БИЛЕТ № 15

Нормативное закрепление состава защищаемой информации; структура перечней сведений, относимых к различным видам тайны.

Состав технических средств обработки, передачи, транспортировки и защиты информации, являющихся объектами защиты.

Рекомендуемый перечень вопросов для внесения на междисциплинарный итоговый государственный экзамен.

Определение и место проблем информационной безопасности в общей совокупности информационных проблем современного общества. Анализ развития подходов к защите информации. Современная постановка задачи защиты информации.

Особенности и состав научно-методологического базиса решения задач защиты информации. Общеметодологические принципы формирования теории защиты информации.

Основное содержание теории защиты информации. Модели систем и процессов защиты информации.

Определение и содержание понятия угрозы информации в современных системах ее обработки. Системная классификация угроз. Система показателей уязвимости информации. Методы и модели оценки уязвимости информации.

Постановка задачи определения требований к защите информации.

Методы оценки параметров защищаемой информации. Факторы, влияющие на требуемый уровень защиты информации.

Определение и общеметодологические принципы построения систем защиты информации. Основы архитектурного построения систем защиты. Типизация и стандартизация систем защиты.

Основные выводы из истории развития теории и практики защиты информации. Перспективы развития теории и практики защиты. Трансформация проблемы защиты информации в проблему обеспечения информационной безопасности.

Основные подходы к оценке и принципы оценки безопасности ИТ, используемые в TCSEC, ITSEC, РД Гостехкомиссии России. Сходство и различия.

Концепция разработки и оценки СЗИ НСД, действующая в России (на основе РД Гостехкомиссии России). Сходство и различия в подходах к оценке безопасности ИТ, изложенных в РД Гостехкомиссии России и «Общих критериях».
Концепция оценки безопасности ИТ, лежащая в основе «Общих критериев». Сходство и различия в подходах к оценке безопасности ИТ, изложенных в РД Гостехкомиссии России и «Общих критериях».
Основные принципы проектирования системы защиты информации от НСД.

Рекомендуемые информационные источники.

Основная литература

Завгородний В.И. Комплексная защита в компьютерных системах: Учебное пособие. – М.: Логос; ПБОЮЛ Н.А.Егоров, 2001. - 264 с.
Райкин И.Л. Информационная безопасность и защита информации: учебник для вузов / НГТУ им. Р.Е. Алексеева. – Нижний Новгород, 2011. – 256 с.

Дополнительная литература

1. Дикарев В.И. и др. Защита объектов и информации от несанкционированного доступа. –
СПб, ―Стройиздат‖. – 2004. – 300 с.

Периодическая литература (журналы)

1. «Информационные технологии»;
2. «Открытые системы»;
3. «Information Security/ Информационная безопасность»;
4. «Проблемы информационной безопасности. Компьютерные системы»;
5. «Информационное общество»;
6. «Информационные процессы».

Адреса сайтов в сети Интернет, где находится информация по содержанию дисциплины и необходимая литература.

1. http://att.nica.ru
2. http://www.edu.ru/
3. http://window.edu.ru/window/library
4. http://www.intuit.ru/catalog/

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению курсового проекта по дисциплине

«**Комплексное обеспечение информационной безопасности автоматизированных систем**»

для студентов специальности

10.05.03 Информационная безопасность автоматизированных систем

Введение

Настоящие рекомендации предназначены для студентов всех форм обучения при выполнении курсовых работ, для руководителей курсовых работ с целью формирования единых требований при разработке и защите работ. Рекомендации содержат предложения по структуре курсовой работы (далее - работа), объему, содержанию, оформлению, процедуре допуска к защите и порядку защиты работ.

Целями выполнения курсовой работы являются:

- обогащение знаний студентов,
- обучение методам теоретического анализа явлений и закономерностей науки,
- выработка навыков применения теоретических знаний к комплексному решению профессиональных задач, использования справочной литературы, методов математической обработки экспериментальных данных, компьютерных технологий.

Системой курсовых работ (проектов) студент подготавливается к выполнению выпускной квалификационной работы.

Перед прочтением Методических указаний ознакомьтесь с основными ошибками, которые допускают студенты, приступая к написанию курсовой работы. Возможно, это мотивирует на более внимательное отношение к требованиям по написанию курсовой работы.

1. Выбрав тему, студент выходит в сеть Интернет и через поисковую систему (Yandex, Google и т.д. – зависит от предпочтений) находит курсовую работу по данной теме, меняет реквизиты, Ф.И.О. автора и сдаёт преподавателю. В результате получает рецензию: «Плагиат. На переработку».
2. Аналогичные действия п.1, но студент подходит к решению проблемы творчески и находит несколько курсовых работ по данной теме. Компонует материал по своему усмотрению и сдает преподавателю под своим авторством. В результате получает рецензию: «Плагиат. На переработку». Почему дана такая рецензия? По трем основным причинам: во-первых, написание курсовых работ – распространённый бизнес в Интернете и качественный материал бесплатно не выкладывают в сети, таким образом, компоновать приходится из «третьесортного сырья»; во-вторых, курсовая уже написана и защищена ранее, то есть она уже устарела и не отражает современных реалий, в-третьих, такие работы редко соответствуют требованиям, предъявляемым кафедрой к курсовым работам.
3. Студент принимает постороннюю помощь в написании работы. Здесь есть несколько аспектов, но следует обратить внимание на два основных. Во-первых, помощь исходит, как правило, от одного физического или юридического лица для группы студентов. В результате преподаватель получает на проверку несколько работ на разные темы, написанные «одной рукой». Формальных причин для отрицательной рецензии у преподавателя нет, особенно если работа выполнена в строгом соответствии с требованиями, но, как показывает практика, защита таких работ проходит безуспешно. Во-вторых, студент, не приложивший усилий к данной работе, как правило, очень плохо в ней ориентируется, особенно, когда преподаватель уточняет аспекты рассматриваемой темы. Но так как Вы уже вышли на защиту, то получаете заслуженную оценку «неудовлетворительно».
4. Вы самостоятельно осуществляете работу, но так же самостоятельно выбираете требования к курсовой работе. Если Вам они нравятся и понятны, то исполняете, а если не нравятся, пропускаете. Это очень распространённая ошибка. Выполнять надо все без исключения требования к курсовой работе. Если в процессе работы возникли вопросы, следует по ним получить консультацию у научного руководителя.

Это краткий перечень основных ошибок, которые недопустимо совершать после прочтения данных Методических указаний.

1. ОРГАНИЗАЦИЯ ВЫПОЛНЕНИЯ И ЗАЩИТЫ КУРСОВОЙ РАБОТЫ

Виды работ по этапам выполнения курсовой работы:

а) Предварительный этап:

- выбор темы курсовой работы и оценка возможности раскрытия данной темы;
- подача заявления на закрепление темы;

б) Основной этап:

- сбор материала;
- оформление курсовой работы;

в) Заключительный этап:

- рецензирование работы руководителем и допуск к защите;
- защита работы.

1.1 Предварительный этап

Темы курсовых работ определяются выпускающей кафедрой. Студенту предоставлено право выбора темы курсовой работы. Задание к выбранной теме выдается руководителем работы (проекта) и регистрируется в кафедральном журнале.

1.2 Основной этап

Составление плана курсовой работы

План курсовой работы представляет собой составленный в определенном порядке перечень глав и развернутый перечень вопросов, которые должны быть освещены. Правильно составленный план работы помогает систематизировать материал, обеспечивает последовательность его изложения. План работы составляется самостоятельно, с учетом замысла и индивидуального подхода. План работы рекомендуется **согласовать с руководителем курсовой работы**. В процессе работы план работы может уточняться.

Подбор литературы

Курсовая работа выполняется на основе глубокого изучения литературных источников. Литература по теме работы может быть подобрана студентом при помощи предметных и алфавитных каталогов библиотек. Для этих целей могут быть использованы каталоги книг, указатели журнальных статей, специальные библиографические справочники, тематические сборники литературы, периодически выпускаемые отдельными издательствами, интернет-сайты официальных организаций.

Проработка источников сопровождается выписками, конспектированием. Выписки из текста делают обычно в виде цитаты. После каждой цитаты приводится ссылка на автора и источник. Поэтому при выписке цитат и конспектировании следует делать ссылки: автор, название издания, место издания, издательство, год издания, номер страницы. Конспект может содержать в себе факты, доказательства, примеры, основные положения и выводы автора, а также личное отношение студента к изученному материалу.

Рациональной и эффективной организации исследовательской деятельности способствует составление студентом собственной картотеки проработанных по теме и смежным вопросам литературных источников. Картотека не только помогает получить представление о степени изученности данной проблемы, но и позволяет работать с литературой более целеустремленно.

Оформление курсовой работы

Оформление проекта или работы осуществляется в соответствии с требованиями положения о выполнении и защите курсовых о выполнении и защите курсовых работ (проектов).

Содержание и структура курсовых работ

Курсовая работа должна содержать элементы новизны, наряду с фундаментальным аспектом должен быть проведен анализ современного состояния изучаемой проблемы, а также отражены региональные особенности. Задание по курсовой работе необходимо индивидуализировать с учетом интересов и способностей студентов.

Курсовая работа должна состоять из введения, теоретической части, эмпирической (практической, расчетно-графической) части, заключения, списка литературы и приложения. В отдельных случаях, в соответствии с тематикой работы, эмпирическая часть может отсутствовать.

Во введении обосновывается актуальность выбранной темы исследования, задачи, цели, новизна, теоретическая и практическая значимость исследования.

Теоретическая часть должна содержать анализ состояния изучаемой проблемы на основе обзора научной, научно-информационной, справочной литературы. Представленный материал должен быть логически связан с целью исследования. В параграфах теоретической части необходимо отражать отдельные компоненты проблемы и завершать их выводами.

Эмпирическая (практическая, расчетно-графическая) часть (при наличии) включает описание системы экспериментального исследования, обоснование методов исследования, анализ результатов экспериментального исследования, схемы, графические и математические способы интерпретации полученных данных, выводы.

Заключение содержит выводы, подтверждающие или опровергающие первоначальные предположения (гипотезы), перспективы дальнейшего изучения проблемы, связь с практикой, анализ реализации целей и задач исследования.

Список литературы должен быть составлен в соответствии с требованиями к оформлению библиографий.

Приложение содержит весь фактический материал экспериментальных исследований (анкеты, опросники, схемы, чертежи, расчетные материалы, карты, рисунки, ответы респондентов и т.д.).

Содержание курсовой работы (проекта) рекомендуется представлять в объеме 20-30 страниц печатного текста. Текст работы должен быть напечатан через 1,5 интервала на одной стороне стандартного листа белой бумаги (А - 4). Текст и другие отпечатанные элементы работы должны быть черными, контуры букв и знаков – четкими, без ореола и затенения. Шрифт TimesNewRoman, кегель 14. Курсив и подчеркивание в работе не допускаются. Названия глав и параграфов выделяются

полужирным шрифтом. Лист с текстом должен иметь поля: слева – 30 мм, справа – 10 мм, сверху – 20 мм, снизу – 20 мм. Нумерация страниц текста делается в правом нижнем углу листа. Проставлять номер страницы необходимо со страницы, где печатается "Введение", на которой ставится цифра "3". После этого нумеруются все страницы, включая приложения.

Между названием главы и названием параграфа этой главы ставится пробел равный двум интервалам, а название параграфа не должно отделяться от текста этого параграфа пробелом. Названия параграфов отделяются от текста предыдущего параграфа пробелом, равным двум интервалам. Каждая глава, а также введение, выводы, предложения и список использованной литературы начинаются с новой страницы. Слово "Глава" не пишется. Главы имеют порядковые номера в пределах всей работы, обозначаемые арабскими цифрами (например: 1,2,3), после которых ставится точка. Слово "параграф" или значок параграфа в названии не ставятся. Параграфы имеют порядковые номера в пределах глав, обозначаемые арабскими цифрами (например: 1.1. и 1.2.). Заголовки глав и параграфов в тексте работы должны располагаться по центру, точку в конце названия главы и параграфа не ставят. Не допускается переносить часть слова в заголовке.

Нумерация таблиц и рисунков может быть сквозной или соотноситься с номером главы и параграфа. Например, если таблица или рисунок включены в текст первого параграфа второй главы, нумерация следующая: Таблица 2.1.1., рис. 2.1.1. Последняя цифра означает порядковый номер таблицы (или рисунка) в данном параграфе. Таблица помещается в качестве следующей страницы после первого упоминания о ней в тексте.

В рамках отведенного для руководства курсовыми работами времени регулярно проводятся индивидуальные консультации. Руководитель работы осуществляет предварительный просмотр выполненных заданий. После проверки выполнения студентом одного этапа работы, руководитель работы разрешает студенту перейти к следующему.

1.3 Заключительный этап

Работа сдается руководителю. Если работа удовлетворяет требованиям, предъявляемым к курсовым работам, она допускается к защите.

Защита курсовой работы является обязательной формой проверки выполнения работы. Защита производится на заседании кафедры, научно-методического семинара кафедры, научной проблемной группы при непосредственном участии руководителя, в присутствии студентов. Результаты наиболее интересных курсовых работ могут быть доложены на научных конференциях.

Защита состоит в коротком докладе студента по выполненной работе и в ответах на вопросы присутствующих на защите.

Результаты защиты курсовой работы, согласно действующему Положению о текущем контроле и промежуточной аттестации, оцениваются дифференцированной отметкой по пятибалльной системе.

Студент, не представивший в установленный срок работу, получивший неудовлетворительную оценку на защите или не явившийся на защиту по неуважительной причине, считается имеющим академическую задолженность.

Для ликвидации академической задолженности студент обязан в установленные сроки представить курсовую работу руководителю и защитить её перед комиссией.

Допуск к защите курсовой работы

Допуск к защите осуществляет научный руководитель курсовой работы.

Работа не допускается к защите, если она не носит самостоятельного характера, списана из литературных источников или у других авторов, если основные вопросы не раскрыты, изложены схематично, фрагментарно, в тексте содержатся ошибки, научный аппарат оформлен неправильно, текст написан небрежно.

Неудовлетворительно выполненная работа подлежит переработке в соответствии с замечаниями преподавателя, содержащимися в отзыве.

При получении допуска к защите студент вправе получить дополнительную консультацию по предстоящей защите.

Курсовая работа, студенту не возвращается и хранится на кафедре в течение 2-х лет.

После получения допуска к защите, студент самостоятельно готовится к защите: составляет текст доклада, реагирует на замечания руководителя.

Подготовка к защите курсовой работы включает устранение ошибок и недостатков, изучение дополнительных источников, готовность объяснить любые приведенные в работе положения.

В ходе защиты курсовой работы задача студента - показать углубленное понимание вопросов конкретной темы, хорошее владение материалом по теме.

Защита работы производится в соответствии с планом приёма защит курсовых работ. С ним можно ознакомиться на стенде кафедры или непосредственно уточнить у научного руководителя время и место защиты.

По результатам защиты курсовой работы в зачётную ведомость (для защиты курсовой

работы) выставляется оценка.

Критерии оценки курсовой работы:

- «**отлично**» выставляется студенту, показавшему глубокие знания, которые применяются при самостоятельном исследовании избранной темы, умение обобщать практический материал и делать на основе анализа выводы. Курсовая работа с оценкой «отлично» может быть рекомендована на конкурс студенческих работ, использована в качестве доклада на научно-студенческой конференции.
- «**хорошо**» выставляется студенту, показавшему в работе и при её защите полное знание материала, всесторонне осветившему вопросы темы, но не полной мере проявившему самостоятельность в исследовании.
- **«удовлетворительно»** выставляется студенту, раскрывшему в работе основные вопросы избранной темы, но не проявившему самостоятельности в анализе или допустившему отдельные неточности содержания работы.
- «**неудовлетворительно»** выставляется студенту, не раскрывшему основные положения избранной темы и допустившему грубые ошибки в содержании работы.

2. СОДЕРЖАНИЕ КУРСОВОЙ РАБОТЫ

2.1 Структурные элементы курсовой работы

Структурными элементами курсовой работы являются:

1) титульный лист,
2) оглавление,
5) введение;
6) основная часть;
7) заключение;
8) список использованных источников;
9) приложения.

Титульный лист является первой страницей курсовой работы.

Оглавление включает введение, наименование всех глав и параграфов, заключение, список использованных источников и приложения с указанием номеров страниц, с которых начинаются эти элементы работы. Следует обратить внимание, что через оглавление прослеживается структура всей работы. Желательно основную часть работы уместить в 2 главы, каждая из которых разбивается на 2-3 параграфа. Глава не может содержать один параграф. Наличие в главе более трех параграфов говорит о поверхностном представлении данных вопросов, так как к работе предъявляются жесткие требования по объему работы.

Введение. Во введении обосновывается **актуальность темы**, **формулируются цель** курсовой работы **и комплекс взаимосвязанных задач**, подлежащих решению в процессе работы, а также представляется **теоретическая и методологическая база.**

Актуальность темы отражает степень важности её раскрытия на данный момент, то есть, почему читателю будет интересно, важно или просто необходимо познакомиться с Вашей работой. Это 2-3 предложения, которые анонсируют Вашу работу. Важно во введении**,** раскрывая актуальность темы, не уйти в раскрытие заявленной проблемы. Не следует писать фразы типа: «Мне эта тема очень интересна, поэтому она актуальна». Здесь необходимо заинтересовать читателя предметно и содержательно, а не своим примером.

Цель работы – это результат, к которому Вы желаете прийти и путь к нему. Цель работы одна. Формулируем её с использованием неопределённой формы глагола: изучить, исследовать, проанализировать, рассмотреть и т.д. Цель вашей курсовой работы скрыта в названии работы.

Задачи работы отражают шаги, делая которые, Вы достигаете цели. Вы должны поставить 6 - 7 задач. Они фактически связаны с параграфами Вашей работы. Задачи формулируются аналогично цели с использованием неопределенной формы глагола: изучить, исследовать, проанализировать, рассмотреть, оценить, выявить и т.д.

Теоретическая и методологическая база подразумевает краткое описание использованных источников с указанием основных авторов. Это «поклон» в адрес людей, чьими трудами Вы воспользовались, а также возможность для специалиста с первого взгляда понять, о чем написана работа и какого подхода к данной проблеме придерживаетесь Вы.

Объем этой части работы 1 лист.

Так как введение – это та часть работы, которая подразумевает 100% самостоятельное изложение, важно не перейти на «ты» в общении с подразумеваемым читателем, то есть **всё изложение материала должно осуществляется в неопределенной форме глагола**. Нельзя употреблять местоимение «я».

Основная часть. Требования к содержанию основной части работы даны ранее.

Заключение. В заключении формулируются краткие выводы, полученные в ходе выполнения поставленных задач и цели. Вы кратко излагаете то, что написали в работе, но это самое главное, что вы хотите донести до читателя, самый «сок» Вашего труда. В заключение можно вынести числовые данные в целях иллюстрации вывода. Они должны отражать цель и задачи исследования, и не быть «вырванными» из работы числами.

Список использованных источников должен содержать сведения об источниках, использованных при выполнении работы.

Приложения. В приложении рекомендуется включать материалы, связанные с выполненной работой, которые по каким-либо признакам не могут быть включены в основную часть.

2.2 Содержание основной части курсовой работы

Теоретический раздел

Раздел должен иметь наименование, отражающее теоретические аспекты темы курсовой работы. В общем случае в этом разделе должны быть отражены:

1) характеристика предмета исследования в соответствии темой курсовой работы, в частности, должен присутствовать анализ понятийной базы по заявленной теме.

2) анализ состояния вопроса, являющегося темой работы, при необходимости – методы анализа.

3) основные подходы к решению проблемы, являющейся темой курсовой работы.

Теоретический раздел должен давать ответы на вопросы, что представляет собой проблема, являющаяся темой курсовой работы.

Объем раздела – 10 - 12 с. В разделе должно быть **не менее двух и не более трех подразделов**.

Аналитический раздел

Наименование данного раздела должно быть связано с анализом состояния предмета исследования, являющегося темой курсовой работы.

Исследование проблемы должно быть целевым и глубоким.

В аналитическом разделе используются различные приемы анализа, указываются источники информации, приводятся аналитические таблицы и расчеты, графические способы отражения результатов анализа, делаются выводы.

В данном разделе обязательно использование не только статистического материала, но и результатов анализа, проведенного специалистами по данному вопросу, которые изложены в источниках периодической печати.

Объем аналитического раздела курсовой работы не должен превышать 10-12 страниц.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Перечень основной литературы:

1. Галатенко В.А. Основы информационной безопасности. – М.: Интернет-Университет Информационных Технологий, 2020.
2. Петраков А.В. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2021.
3. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. – М.: ДМК Пресс, 2019.
4. Лопатин В.Н. Информационная безопасность России. – СПб.: Юридический центр Пресс, 2018.
5. Белов Е.Б., Лось В.П. Основы информационной безопасности. – М.: Горячая линия – Телеком, 2020.

Перечень дополнительной литературы:

6. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации".
7. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных".
8. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности".
9. Приказы ФСТЭК России
10. ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения".
11. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций".