

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 «Информационная безопасность»

для студентов направления подготовки
09.03.02 «Информационные системы и технологии»
Профиль «Прикладное программирование и интернет-технологии»

Ставрополь, 2026

Оглавление

Лабораторная работа 1. Сущность и задачи комплексной системы защиты информации	3
Лабораторная работа 2. Методологические основы комплексной системы защиты информации	23
Лабораторная работа 3. Определение состава защищаемой информации.....	39
Лабораторная работа 4. Требования к системам защиты информации.....	46
Лабораторная работа 5. Оценка качества комплексной системы информационной безопасности	55
Лабораторная работа 6. Эксплуатационная документация КСИБ	65
Лабораторная работа 7. Особенности эксплуатации КСИБ на объекте защиты	101
Лабораторная работа 8. Организационно-функциональные задачи службы безопасности	119
Лабораторная работа 9. Управление комплексной системой защиты информации.....	147

Лабораторная работа 1.

Сущность и задачи комплексной системы защиты 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:

1. Формирование требований к защите информации, содержащейся в информационной системе.
2. Разработка КСЗИ информационной системы.
3. Внедрение КСЗИ информационной системы.
4. Аттестация информационной системы по требованиям защиты информации (далее - аттестация информационной системы) и ввод ее в действие.
5. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы.
6. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

1. Формирование требований к защите информации, содержащейся в 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:

1. Анализ целей создания информационной системы и задач, решаемых этой информационной системой.
2. Определение информации, подлежащей обработке в информационной системе.
3. Анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система.
4. 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 её 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:

1. Проектирование КСЗИ информационной системы.
2. Разработку эксплуатационной документации на систему защиты информации информационной системы.
3. 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:

1. Установку и настройку средств защиты информации в информационной системе.

2. 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).

3. Внедрение организационных мер защиты информации.

4. Предварительные испытания КСЗИ информационной системы.

5. Опытную эксплуатацию КСЗИ информационной системы.

6. Анализ уязвимостей информационной системы и принятие мер защиты информации по их устранению.

7. 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.

3.4. 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.

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

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

4. Аттестация информационной системы и ввод ее в действие

В 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 владельцем 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);

- информирование пользователей об угрозах безопасности 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 ее 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 владельцем 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:

1. Архивирование информации, содержащейся в информационной системе.
2. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

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

6.2. 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.

Оборудование и материалы

Аппаратура. Для выполнения лабораторной работы необходим персональный компьютер со следующими характеристиками: процессор с тактовой частотой 3000МГц и выше, оперативная память – не менее 4 Гб и более, свободное дисковое пространство – не менее 1000 Мб, устройство для чтения компакт-дисков, монитор типа Super VGA (число цветов – 65535).

Программное обеспечение. Для выполнения лабораторной работы необходима операционная система XP Professional и выше, библиотека Microsoft .NET Framework версии 1.1 или выше, антивирусное ПО.

Указания по технике безопасности

При выполнении лабораторной работы **запрещается**:

- самостоятельно производить ремонт персонального компьютера, а также установку и удаление имеющегося программного обеспечения;
- нарушать общепринятые правила техники безопасности при работе с электрооборудованием, в частности, касаться электрических розеток металлическими предметами и т.д.;
- принимать пищу, напитки и сорить на рабочем месте пользователя персонального компьютера.

В случае неисправности персонального компьютера необходимо **немедленно** сообщить об этом обслуживающему персоналу лаборатории (системному администратору, оператору).

Содержание отчета

1. Титульная страница отчета.
2. Цель лабораторной работы.
3. Ответы на контрольные вопросы.
4. Описание выполненной работы.
5. Вывод.

Контрольные вопросы

1. Перечислите основные этапы построения КСЗИ.
2. Назовите ГОСТ с учётом которых должны быть разработаны требования к системе защиты информации.
3. Перечислите основные понятия которые будут определены при проектировании КСЗИ.
4. Перечислите основное содержание эксплуатационной документации КСЗИ.
5. Перечислите этапы внедрения системы защиты информации.
6. 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

Список литературы

1. 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.

http://old.biblioclub.ru/93275_Metody_i_sredstva_inzhenerno_tekhnicheskoi_zaschity_informatsii_uchebnoe_posobie.html

2. 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.)

Лабораторная работа 2.

Методологические основы комплексной системы защиты информации

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 проводиться 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 информации 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 с 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 и 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).

В качестве заявителей могут выступать заказчики, владельцы или разработчики аттестуемых объектов информатизации.

В 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", о 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 и 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:

1. 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.

2. предварительное ознакомление с аттестуемым объектом – производится в случае недостаточности предоставленных заявителем данных до начала аттестационных испытаний;

3. испытание в испытательных лабораториях несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте.

4. 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.

5. 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.

6. проведение аттестационных испытаний объекта информатизации. В 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 объекте,

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.

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

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

9. 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 с 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.

Оборудование и материалы

Аппаратура. Для выполнения лабораторной работы необходим персональный компьютер со следующими характеристиками: процессор с тактовой частотой 3000МГц и выше, оперативная память – не менее 4 Гб и более, свободное дисковое пространство – не менее 1000 Мб, устройство для чтения компакт-дисков, монитор типа Super VGA (число цветов – 65535).

Программное обеспечение. Для выполнения лабораторной работы необходима операционная система XP Professional и выше, библиотека Microsoft .NET Framework версии 1.1 или выше, антивирусное ПО.

Указания по технике безопасности

При выполнении лабораторной работы **запрещается:**

- самостоятельно производить ремонт персонального компьютера, а также установку и удаление имеющегося программного обеспечения;
- нарушать общепринятые правила техники безопасности при работе с электрооборудованием, в частности, касаться электрических розеток металлическими предметами и т.д.;
- принимать пищу, напитки и сорить на рабочем месте пользователя персонального компьютера.

В случае неисправности персонального компьютера необходимо **немедленно** сообщить об этом обслуживающему персоналу лаборатории (системному администратору, оператору).

Практическое задание

1. Написать отчёт исследования предприятия, закреплённого на ЛР1, содержащий общие сведения о предприятии, о его деятельности и организационной структуре.

2. 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

Содержание отчета

1. Титульная страница отчета.
2. Цель лабораторной работы.
3. Ответы на контрольные вопросы.
4. Описание выполненной работы.
5. Вывод.

Контрольные вопросы

1. Какие существуют виды обследования защищённости?
2. Что должен содержать аттестат соответствия?
3. Назовите порядок проведения аттестации объектов информатизации по требованиям безопасности информации?
4. Какие документы предоставляет заявитель Для проведения испытаний органу по аттестации?
5. Какие функции осуществляет ФСТЭК в рамках системы аттестации?

Список литературы

1. 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.
2. Сергеева Ю. С. Защита информации. Конспект лекций. Учебное пособие. - М.: А-Приор, 2011. - 128 с.
http://old.biblioclub.ru/72670_Zaschita_informatsii_Konspekt_lektsii_Uchebnoe_posobie.html
3. Сычев Ю. Н., Основы информационной безопасности. Учебно-практическое пособие - М.: Евразийский открытый институт, 2010. - 328 с.

http://old.biblioclub.ru/90790_Osnovy_informatsionnoi_bezopasnosti_Uchebno_prakticheskoe_posobie.html

4. 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.
http://old.biblioclub.ru/86475_Zaschita_kompyuternoi_informatsii_Effektivnye_metody_i_sredstva.html

Лабораторная работа 3.

Определение состава защищаемой информации

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:

1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

2) требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Уровень защищённости 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 защищённости 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 Состав 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:

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

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

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

4. 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».

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

6. «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.

7. «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.

8. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

9. «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».

Оборудование и материалы

Аппаратура. Для выполнения лабораторной работы необходим персональный компьютер со следующими характеристиками: процессор с тактовой частотой 3000МГц и выше, оперативная память – не менее 4 Гб и более, свободное дисковое пространство – не менее 1000 Мб, устройство для чтения компакт-дисков, монитор типа Super VGA (число цветов – 65535).

Программное обеспечение. Для выполнения лабораторной работы необходима операционная система XP Professional и выше, библиотека Microsoft .NET Framework версии 1.1 или выше, антивирусное ПО.

Указания по технике безопасности

При выполнении лабораторной работы **запрещается:**

- самостоятельно производить ремонт персонального компьютера, а также установку и удаление имеющегося программного обеспечения;
- нарушать общепринятые правила техники безопасности при работе с электрооборудованием, в частности, касаться электрических розеток металлическими предметами и т.д.;
- принимать пищу, напитки и сорить на рабочем месте пользователя персонального компьютера.

В случае неисправности персонального компьютера необходимо **немедленно** сообщить об этом обслуживающему персоналу лаборатории (системному администратору, оператору).

Практическое задание

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

Содержание отчета

1. Титульная страница отчета.
2. Цель лабораторной работы.
3. Ответы на контрольные вопросы.
4. Описание выполненной работы.
5. Вывод.

Контрольные вопросы

1. Назовите закон о защите персональных данных.
2. Каким документом определяются требования к защите персональных данных?
3. Назовите перечень документов используемых для защиты персональных данных.
4. Назовите документ регламентирующий использование криптографических средств защиты в информационных системах.

Список литературы

1. <http://www.intuit.ru> – Сайт национального открытого университета «Интуит»
2. <http://www.citforum.ru> – Сайт центра информационных технологий
3. <http://www.consultant.ru/> - Нормативно-правовая документация

Лабораторная работа 4.

Требования к системам защиты информации

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, её 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:

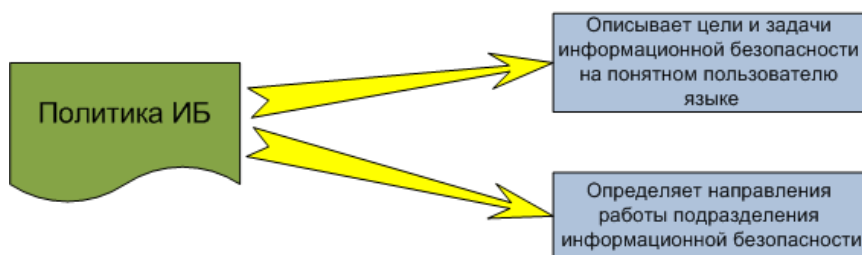
- непротиворечивой – разные документы не должны по разному описывать подходы к одному и тому же процессу обработки информации
- не запрещала необходимые действия – в таком случае неизбежные массовые нарушения приведут к дискредитации политики информационной безопасности среди пользователей
- не налагала невыполнимых обязанностей и требований.

В организации должно быть назначено лицо, ответственное за политику безопасности, отвечающее за её 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.

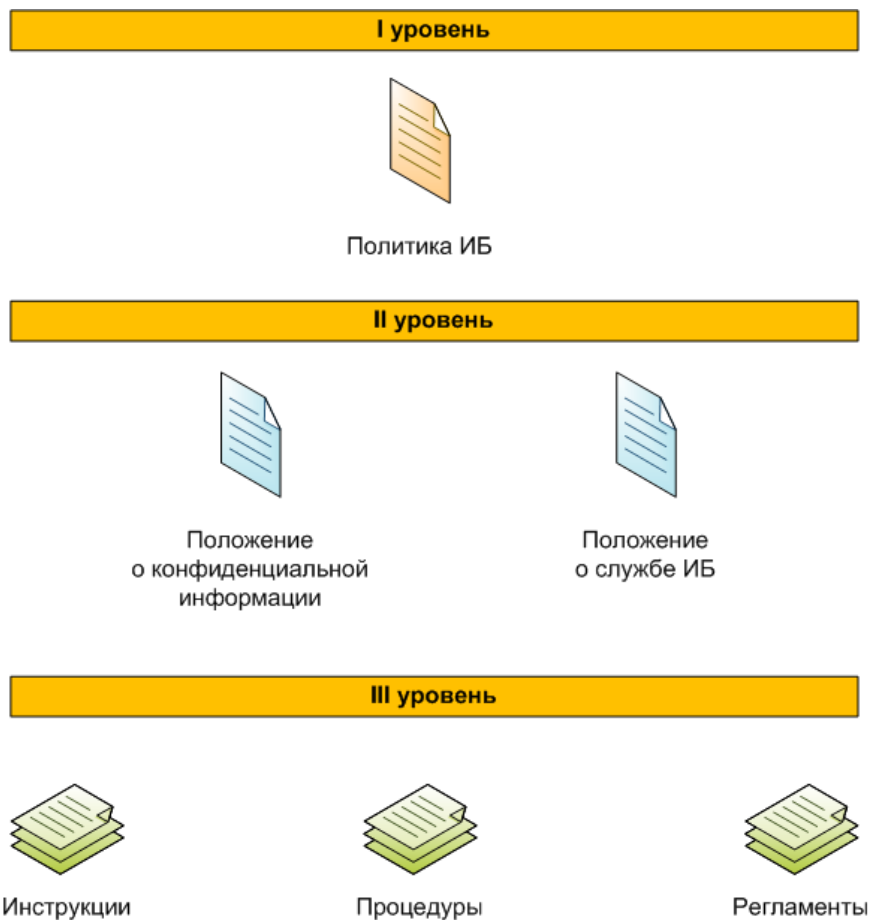


Конечный документ должен удовлетворять следующим требованиям:

– 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 её 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

Оборудование и материалы

Аппаратура. Для выполнения лабораторной работы необходим персональный компьютер со следующими характеристиками: процессор с тактовой частотой 3000МГц и выше, оперативная память – не менее 4 Гб и более, свободное дисковое пространство – не менее 1000 Мб, устройство для чтения компакт-дисков, монитор типа Super VGA (число цветов – 65535).

Программное обеспечение. Для выполнения лабораторной работы необходима операционная система XP Professional и выше, библиотека Microsoft .NET Framework версии 1.1 или выше, антивирусное ПО.

Указания по технике безопасности

При выполнении лабораторной работы **запрещается:**

- самостоятельно производить ремонт персонального компьютера, а также установку и удаление имеющегося программного обеспечения;
- нарушать общепринятые правила техники безопасности при работе с электрооборудованием, в частности, касаться электрических розеток металлическими предметами и т.д.;
- принимать пищу, напитки и сорить на рабочем месте пользователя персонального компьютера.

В случае неисправности персонального компьютера необходимо **немедленно** сообщить об этом обслуживающему персоналу лаборатории (системному администратору, оператору).

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.

Содержание отчета

1. Титульная страница отчета.
2. Цель лабораторной работы.
3. Ответы на контрольные вопросы.
4. Описание выполненной работы.
5. Вывод.

Контрольные вопросы

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

Список литературы

1. 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.
http://old.biblioclub.ru/93349_Razrabotka_sistemy_tekhnicheskoi_zaschity_informatsii_uchebnoe_posobie.html
2. Чипига, А. Ф. Информационная безопасность автоматизированных систем : учеб. пособие / А. Ф. Чипига. – М. : Гелиос АРВ, 2010. – 336 с.
3. Сергеева Ю. С. Защита информации. Конспект лекций. Учебное пособие. - М.: А-Приор, 2011. - 128 с.
http://old.biblioclub.ru/72670_Zaschita_informatsii_Konspekt_lektsii_Uchebnoe_posobie.html

obie.html

Лабораторная работа 5.

Оценка качества комплексной системы информационной безопасности

Цель работы: изучить методику составления плана мероприятий по улучшению защищённости 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 технологическими 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.

Оборудование и материалы

Аппаратура. Для выполнения лабораторной работы необходим персональный компьютер со следующими характеристиками: процессор с тактовой частотой 3000МГц и выше, оперативная память – не менее 4 Гб и более, свободное дисковое пространство – не менее 1000 Мб, устройство для чтения компакт-дисков, монитор типа Super VGA (число цветов – 65535).

Программное обеспечение. Для выполнения лабораторной работы необходима операционная система XP Professional и выше, библиотека Microsoft .NET Framework версии 1.1 или выше, антивирусное ПО.

Указания по технике безопасности

При выполнении лабораторной работы **запрещается:**

- самостоятельно производить ремонт персонального компьютера, а также установку и удаление имеющегося программного обеспечения;
- нарушать общепринятые правила техники безопасности при работе с электрооборудованием, в частности, касаться электрических розеток металлическими предметами и т.д.;

– принимать пищу, напитки и сорить на рабочем месте пользователя персонального компьютера.

В случае неисправности персонального компьютера необходимо **немедленно** сообщить об этом обслуживающему персоналу лаборатории (системному администратору, оператору).

Практическое задание

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

Содержание отчета

1. Титульная страница отчета.
2. Цель лабораторной работы.
3. Ответы на контрольные вопросы.
4. Описание выполненной работы.
5. Вывод.

Контрольные вопросы

1. Дайте определение объекта информатизации.
2. Какая главная цель создания СЗИ?
3. Назовите последовательность шагов для улучшения защищенности объекта информатизации.
4. Какие исходные данные используются для составления плана по улучшению защищённости объекта информатизации?
5. Какими документами должен руководствоваться специалист по защите информации при составлении плана мероприятий по улучшению защищённости объекта информатизации?

Список литературы

1. 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.

http://old.biblioclub.ru/86475_Zaschita_kompyuternoi_informatsii_Effektivnye_mety_i_sredstva.html

2. 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.
http://old.biblioclub.ru/93275_Metody_i_sredstva_inzhenerno_tekhnicheskoi_zaschity_informatsii_uchebnoe_posobie.html

3. 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.

Лабораторная работа 6.

Эксплуатационная документация КСИБ

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 распределенной 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. *Носителем идей нового подхода к организации вычислительного 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.

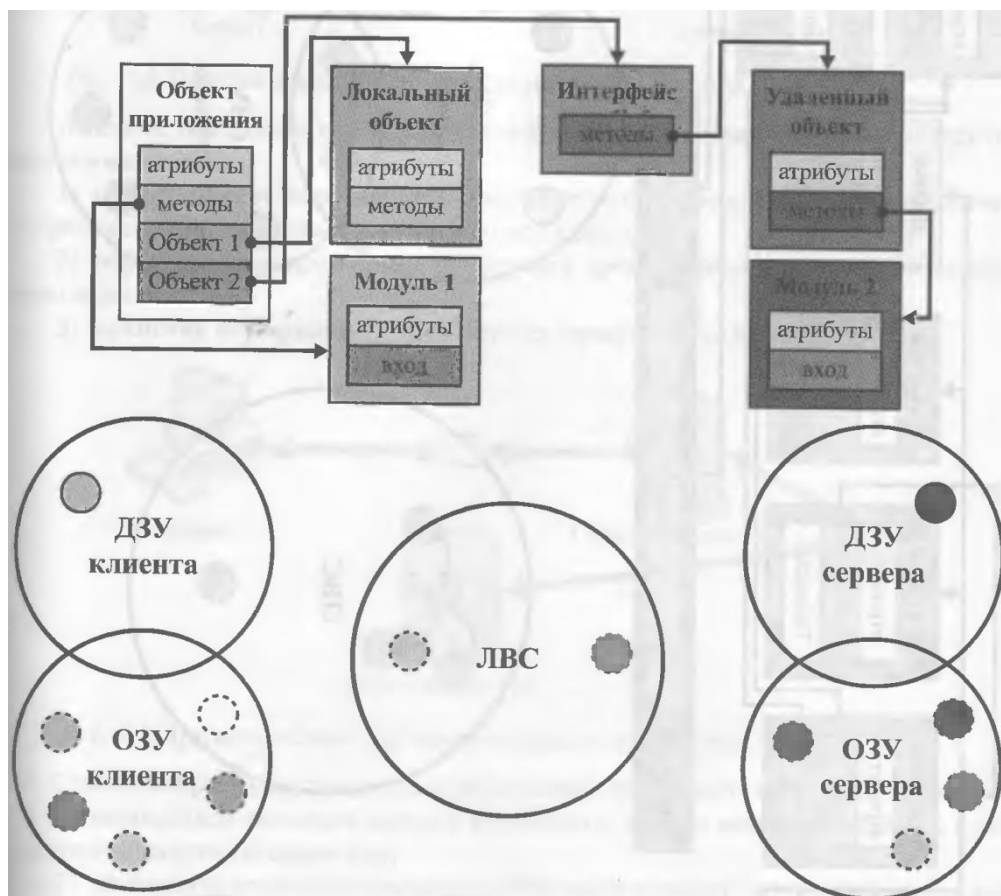


Рисунок 1.1. Структура объектов сетевого приложения

Наибольшая концентрация объектов наблюдается в оперативной памяти сервера баз данных.

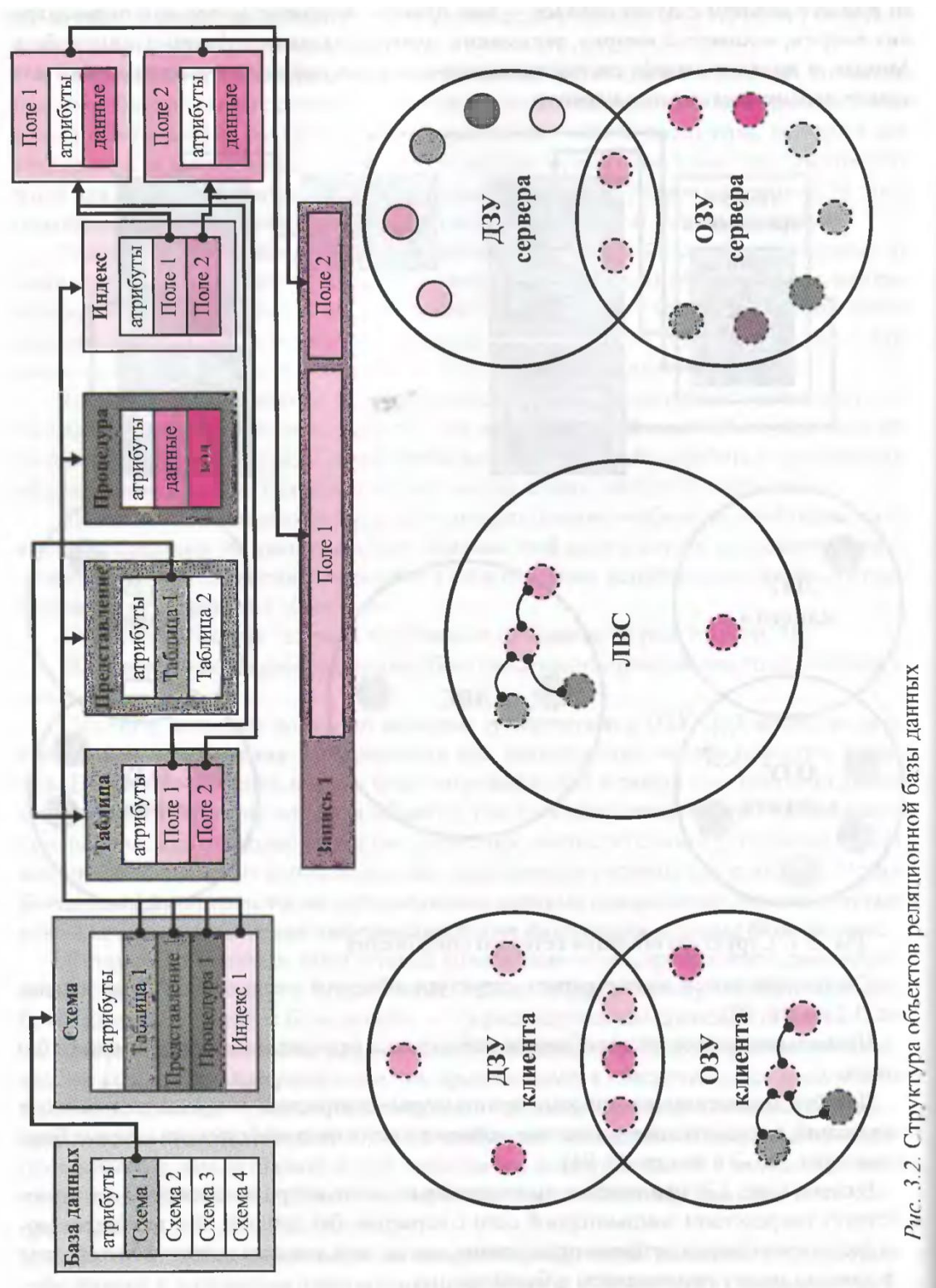


Рис. 3.2. Структура объектов реляционной базы данных

Рисунок 1.2. Структура объектов реляционной базы 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.

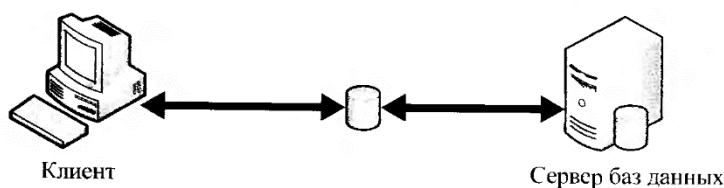


Рисунок 1.3. Простая схема организации сетевого приложения

На схеме, показанной на рис. 1.4, мы наблюдаем декомпозицию задачи на три независимых процесса:

- 1) представление информации – реализуется программными средствами сетевого приложения, выполняемыми на компьютере клиента;
- 2) обработка информации – реализуется программным обеспечением сервера приложения;
- 3) хранение информации – реализуется сервером базы данных.

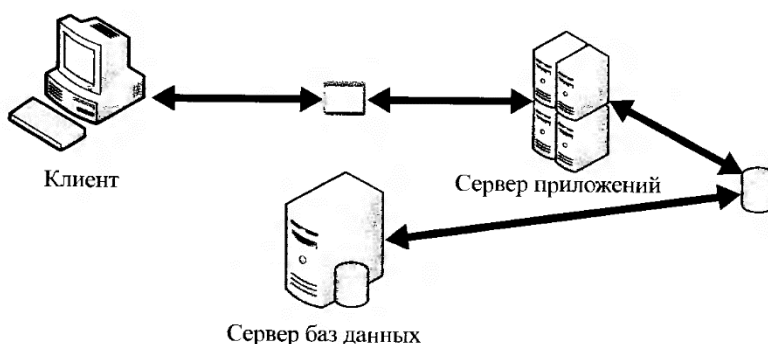


Рисунок 1.4. Три независимых процесса в сетевом приложении

Главными преимуществами такой архитектуры приложения являются:

- 1) независимая эволюция каждого компонента, которая может происходить в разное время с различной скоростью;

2) повышение производительности за счет специализации и оптимизации каждого вычислительного устройства на решении узкой, относительно самостоятельной задачи;

3) 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 и Web-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 Internet Explorer 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.

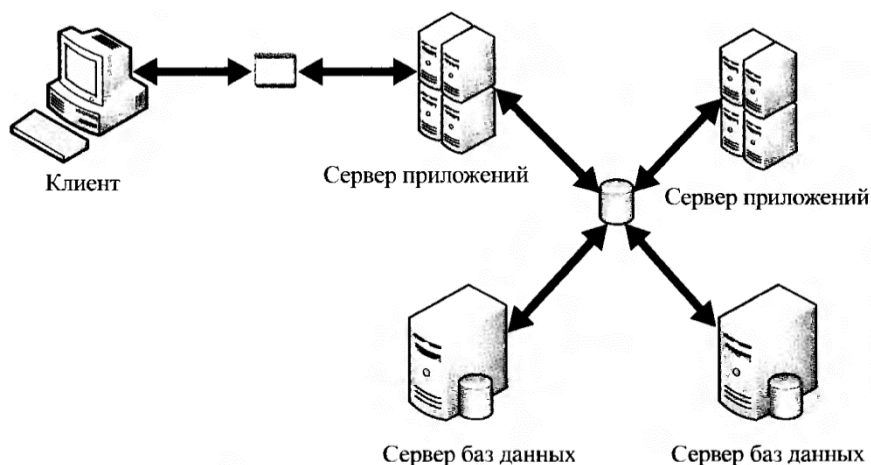


Рисунок 1.5. Нарращивание возможностей сетевого приложения

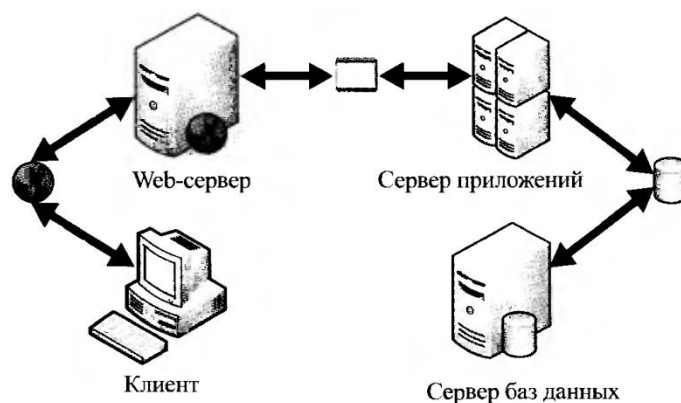


Рисунок 1.6. Разделение задачи представления информации между клиентом сетевого приложения и Web-сервером.

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.

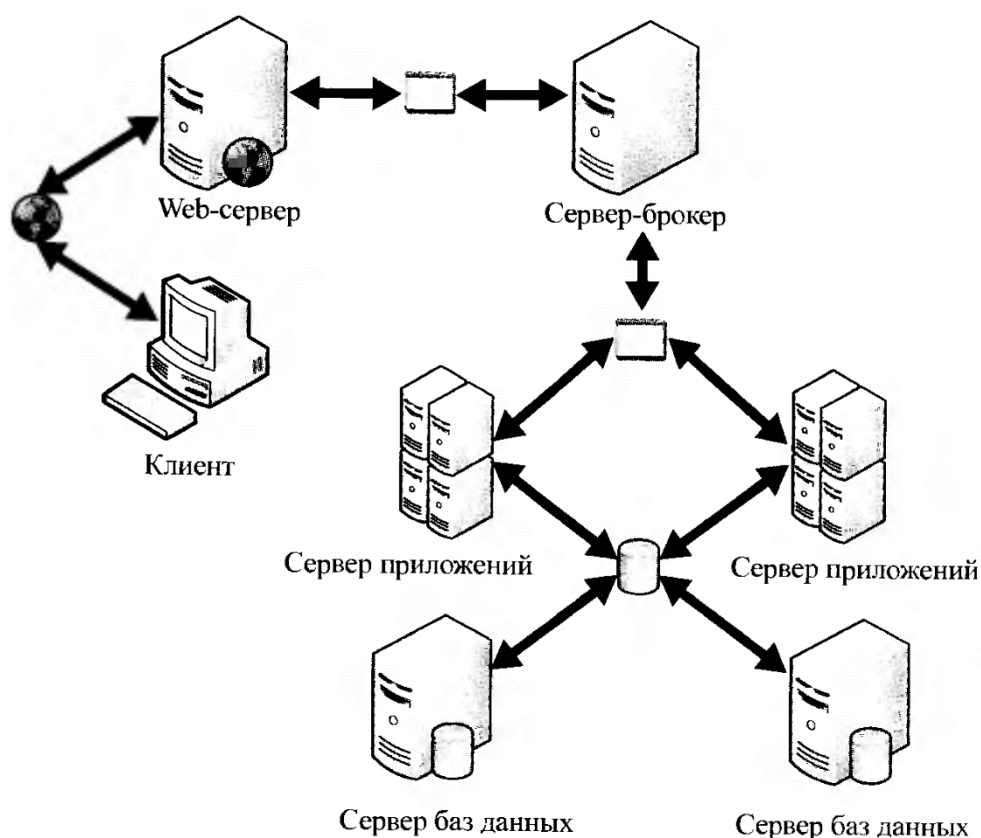


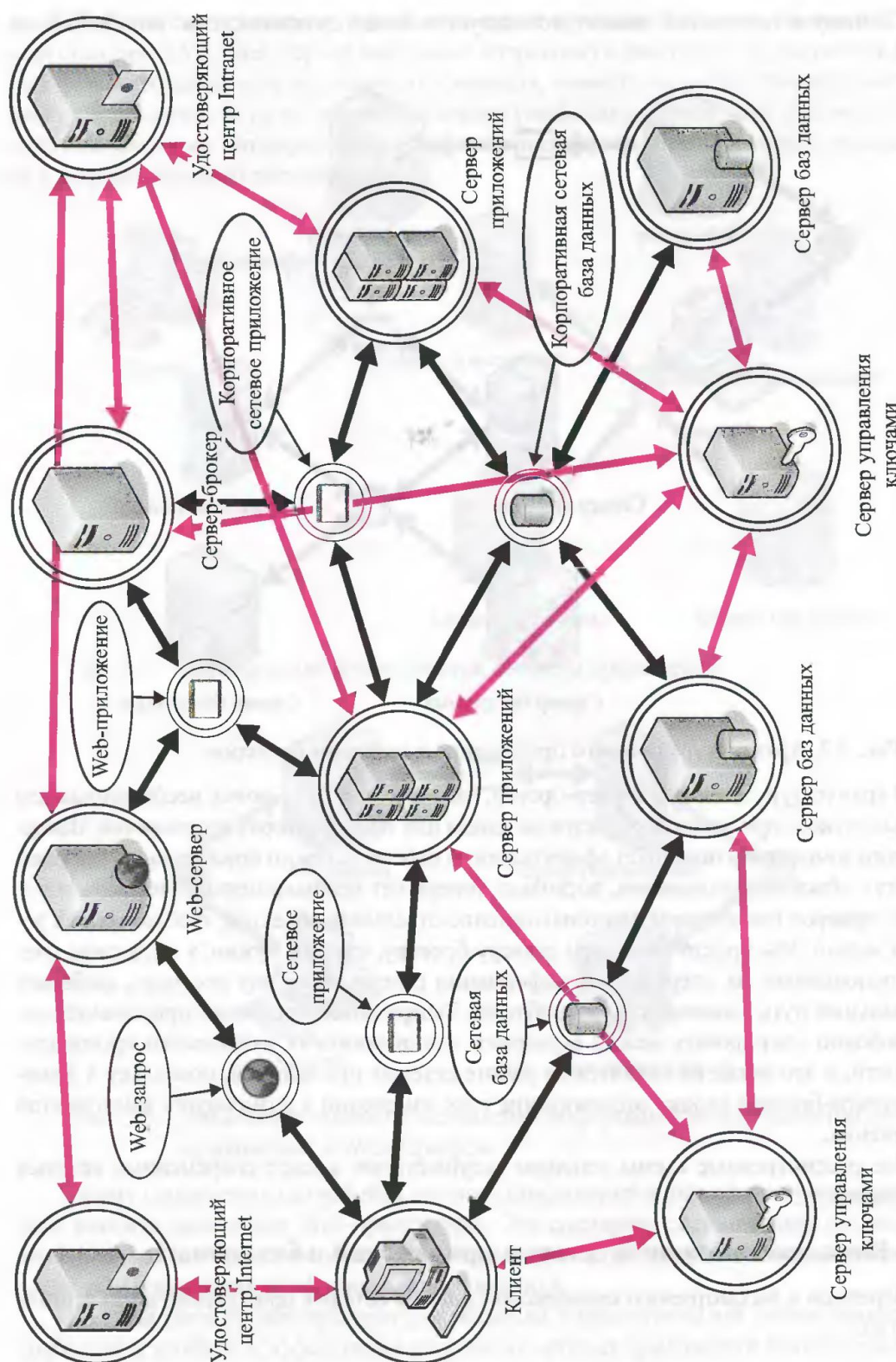
Рисунок 1.7. Архитектура сетевого приложения с сервером-брокером.

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).



Выполним разбиение на отдельные контуры защиты. Начнем с рассмотрения различных зон ЛВС (рис. 1.9).

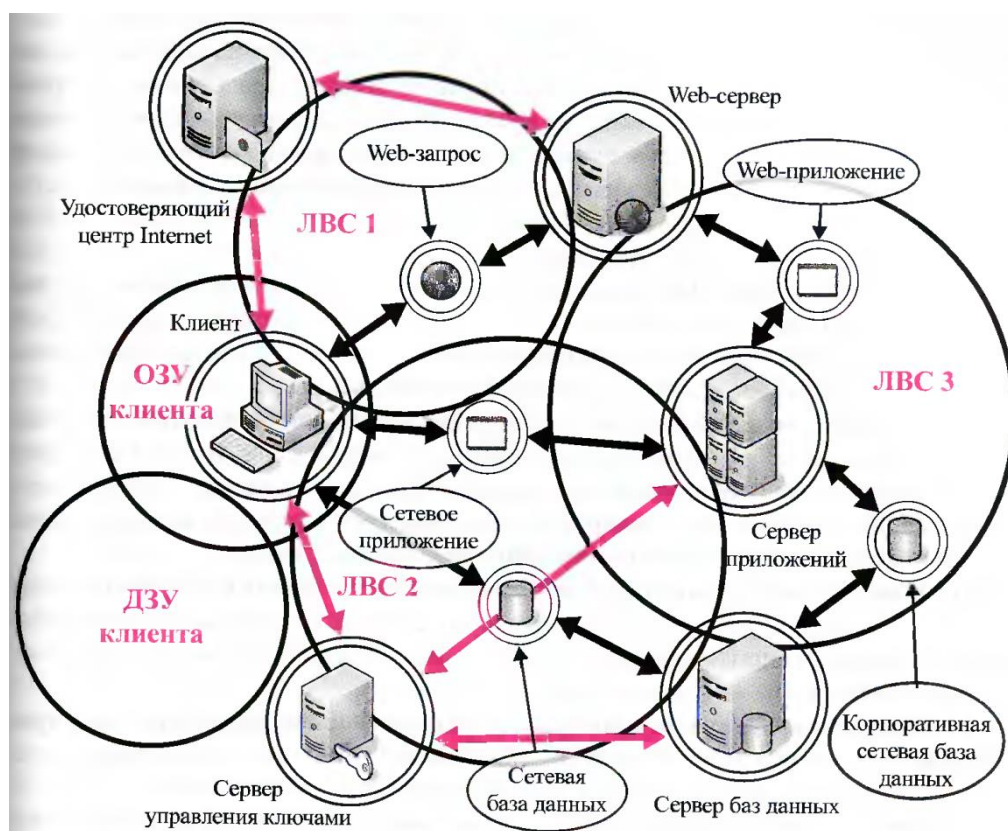


Рисунок 1.9. Различные зоны ЛВС

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; электронные 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:

1) 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;

2) 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;

3) 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;

4) 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:

1) использование уязвимостей программного обеспечения сетевого приложения; цель: путем перехвата управления внедрить в исполняемые процессы вредоносное программное обеспечение с последующим проникновением его в зону ДЗУ и имплантацией в программную среду вычислительной системы;

2) хищение реквизитов доступа к сетевым базам данных и приложениям; цель: обнаружить в оперативной памяти структуры, содержащие критическую информацию – реквизиты доступа пользователя, и перенести ее в область, потенциально доступную злоумышленнику; реализуется через программные закладки и уязвимости программного обеспечения;

3) 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;

4) перехват электронных документов; цель: используя архитектурные особенности унифицированных клиентов сетевых приложений (например стандартного обозревателя `lplshel`), получить доступ к классифицированной информации в виде электронных документов, «осевших» в накопительных областях (кэшах);

5) подмена загружаемых модулей; цель: вынудить клиентское программное обеспечение выполнить загрузку исполняемого модуля, навязанного злоумышленником;

6) 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 защиты 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:

1) перехват данных; цель: восстановить информационные объекты из перехваченных сетевых пакетов с последующим извлечением ценной информации на вычислительных средствах злоумышленника;

2) 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;

3) блокирование клиента сетевого приложения; цель: используя уязвимости программного обеспечения, особенности архитектуры и топологии телекоммуникационной системы, прекратить работу сетевого приложения;

4) 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 корпоративных 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:

- 1) модификация сценариев Web-приложений; цель: используя уязвимости программного обеспечения, ошибки конфигурации и программные закладки, внедрить в сетевое приложение объекты злоумышленника;
- 2) модификация модулей программного обеспечения и файлов конфигураций Web-сервера; цель: используя уязвимости программного обеспечения, ошибки конфигурирования или программные закладки, получить контроль над Web-сервером;

3) хищение реквизитов доступа из файлов конфигурации; цель: извлечь или восстановить из файлов конфигурации Web-приложения критическую информацию, позволяющую получить доступ к серверу приложений или серверу-брокеру от лица санкционированного пользователя.

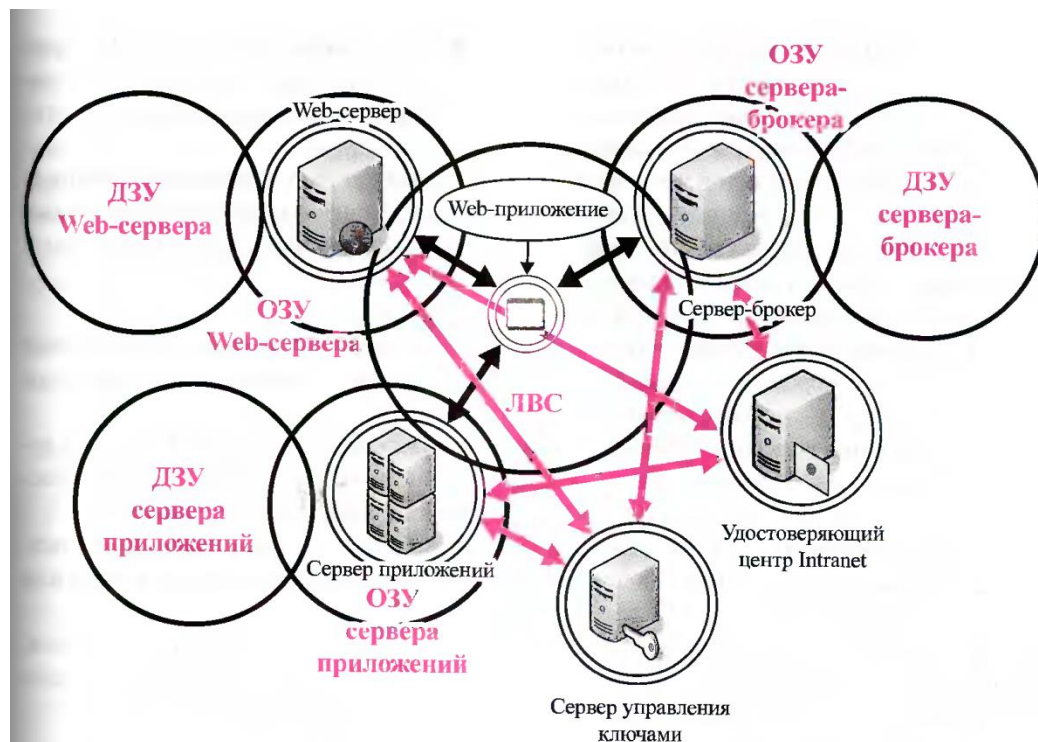


Рисунок 1.10. Взаимодействие средств представления информации со средствами ее обработки

Зона ОЗУ Web-сервера подвержена следующим нападениям:

- 1) использование уязвимостей программного обеспечения; цель: захват контроля над Web-сервером через уязвимости программного обеспечения, ошибки конфигурации или внедрение программных закладок;
- 2) 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;
- 3) 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;

4) 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:

1) 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;

2) 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:

1) использование уязвимостей программного обеспечения; цель: установление контроля над сервером приложений путем воздействия на уязвимости программного обеспечения и ошибки конфигурации;

2) 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;

3) подавление средств защиты; цель: используя архитектурные особенности реализации, уязвимости встроенных и прицепных средств защиты, вывести их из строя или снизить эффективность;

4) 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:

1) модификация исполняемых модулей и файлов конфигурации сервера- брокера; цель: путем модификации программного обеспечения или файлов конфигурации установить контроль над сервером-брокером;

2) модификация базы данных размещения объектов сетевых приложений.

цель: изменить топологию связей объектов сетевого приложения, внедрить объекты злоумышленника.

Типовые нападения на зону ОЗУ сервера-брокера:

1) использование уязвимостей программного обеспечения; цель: воздействуя н.; уязвимости программного обеспечения, ошибки конфигурации или внедряя программные закладки, установить контроль над сервером-брокером в интересах злоумышленника;

2) 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 образуют 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.

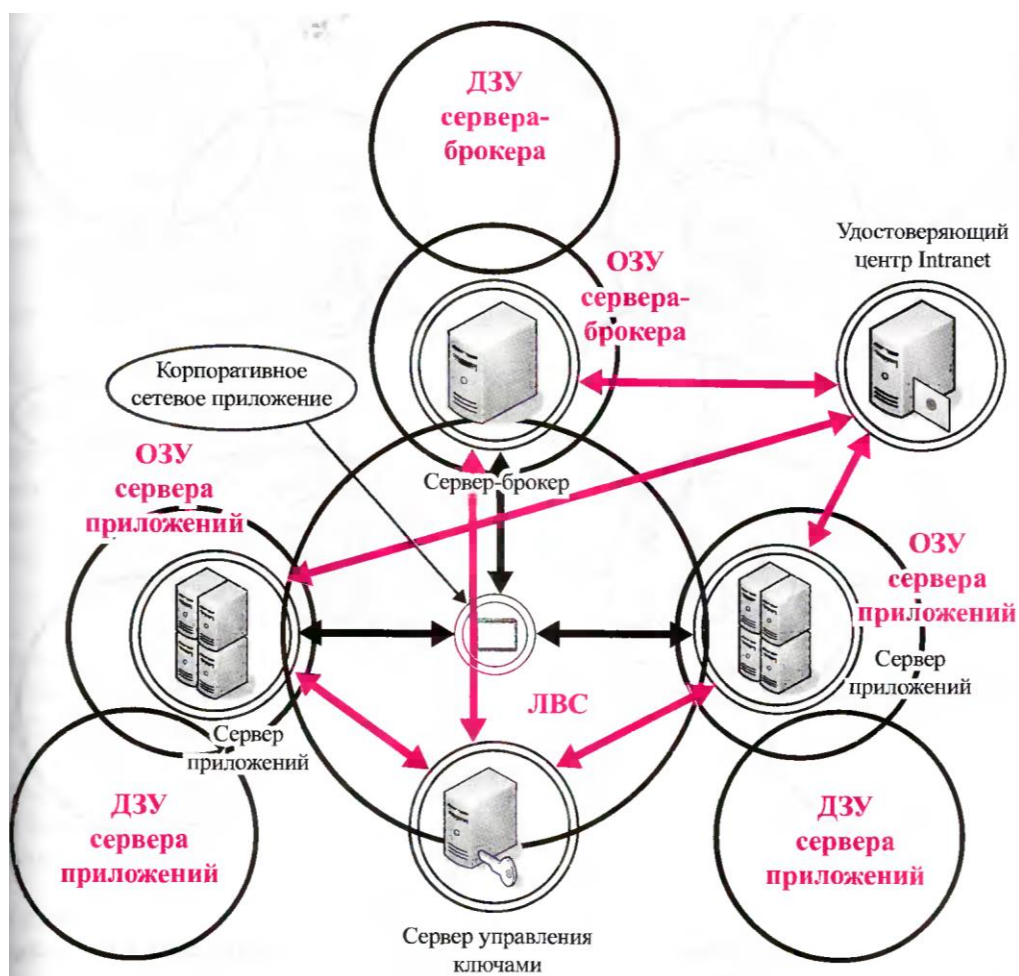


Рисунок 1.11. Защита объектов подсистемы обработки информации

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, немислимо обойтись без средств криптографической защиты.

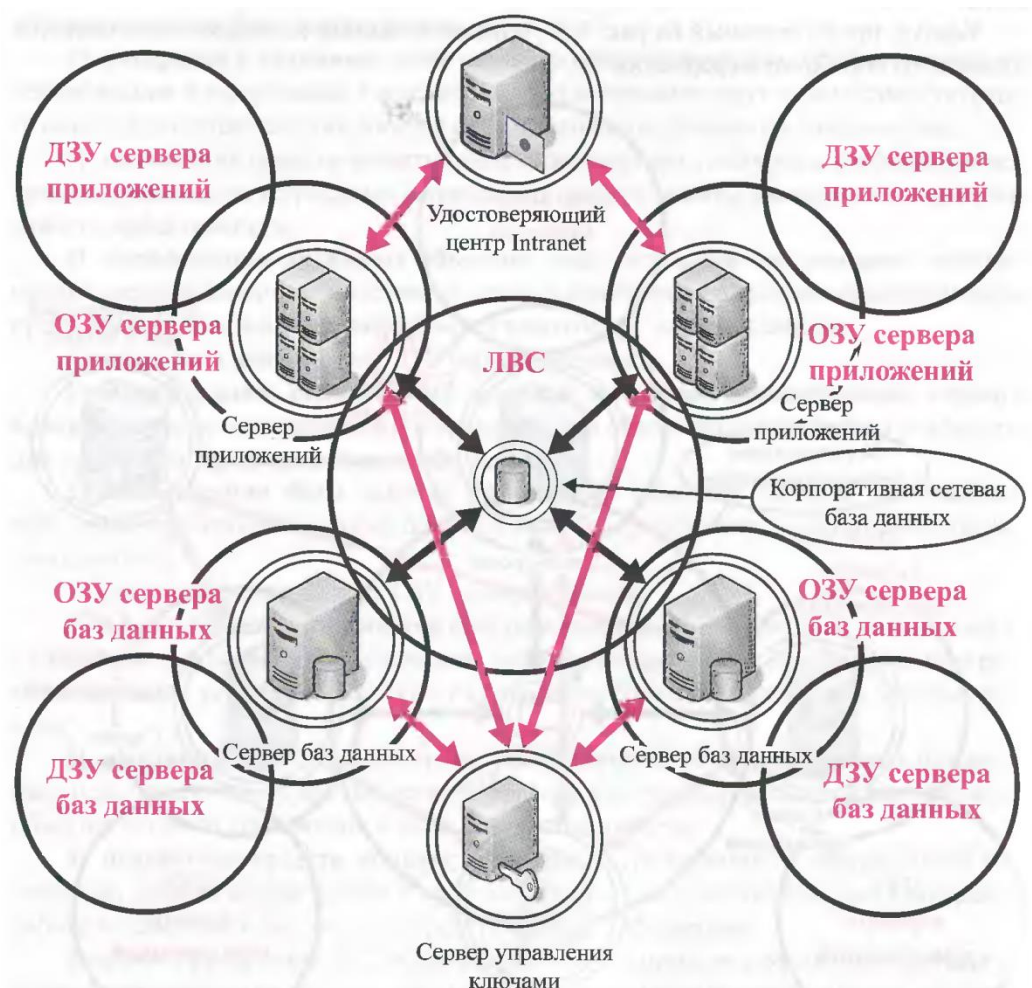


Рисунок 1.12. Защита взаимодействия подсистемы обработки информации с подсистемой хранения

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:

- 1) перехват данных; цель: восстановить из перехваченных сетевых пакетов сеансы удаленного вызова процедур и функций, а также извлечь информацию о переданных для обработки и полученных после нее данных;
- 2) 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;
- 3) блокирование сетевых приложений: цель: используя архитектурные особенности, 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:

1) 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 объему. Избирательные права характеризуются значительной гибкостью;

2) 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;

3) для реализации избирательного принципа предусмотрены следующие методы. В 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, чаще всего, в специальном кодированном виде и известны только самим пользователям;

4) 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;

5) привилегии или полномочия пользователей или групп – это набор действий (операций), которые они могут выполнять над объектами БД;

6) 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;

7) пользователю может быть назначена одна или несколько ролей;

8) 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 процессу информационной системы соответствует набор действий, которые он может выполнять 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 или администратор сервера БД. Традиционно только этот тип пользователей может создавать 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.

В ряде СУБД вводится следующий уровень иерархии пользователей – администратор БД. В этих СУБД один сервер может управлять множеством СУБД (например MSSQLServer? Sybase).

В СУБД Oracle применяется однобазовая архитектура, поэтому там вводится понятие подсхемы – части общей схемы БД, и вводится пользователь, имеющий доступ к подсхеме.

В 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 пользователя> 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 user1, user2 и user3. Все они являются пользователями одной БД.

User1 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 user3 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 user1 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 Tab1 в отсутствие владельца объекта пользователя user1. Поэтому в случае появления нового оператора пользователя user5 он может назначить ему права на ввод новых строк в таблицу командой

```
GRANT INSERT ON Tab1 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 Tab1 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, эффективный метод 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 Tab1
```

```
TO user4 CASCADE
```

будут отменены привилегии и пользователя user5, которому пользователь user4 успел присвоить привилегии.

Параметр RESTRICT ограничивает отмену привилегий только пользователем, непосредственно упомянутому в операторе REVOKE. Но при наличии делегированных привилегий этот оператор не будет выполнен. Так, например, операция:

```
REVOKE ALL PRIVILEGES ON Tab1
```

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 Tab1

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 user1
```

В этом случае пользователь user1 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.

В 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:

- 1) стандартный (standard);
- 2) интегрированный (integratedsecurity);
- 3) смешанный (mixed).

Стандартный режим защиты предполагает, что каждый пользователь должен иметь учетную запись как пользователь домена NT Server. Учетная запись пользователя домена [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.

В случае смешанного режима часть пользователей может быть подключена к серверу с использованием стандартного режима, а часть – с использованием интегрированного режима.

В 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.

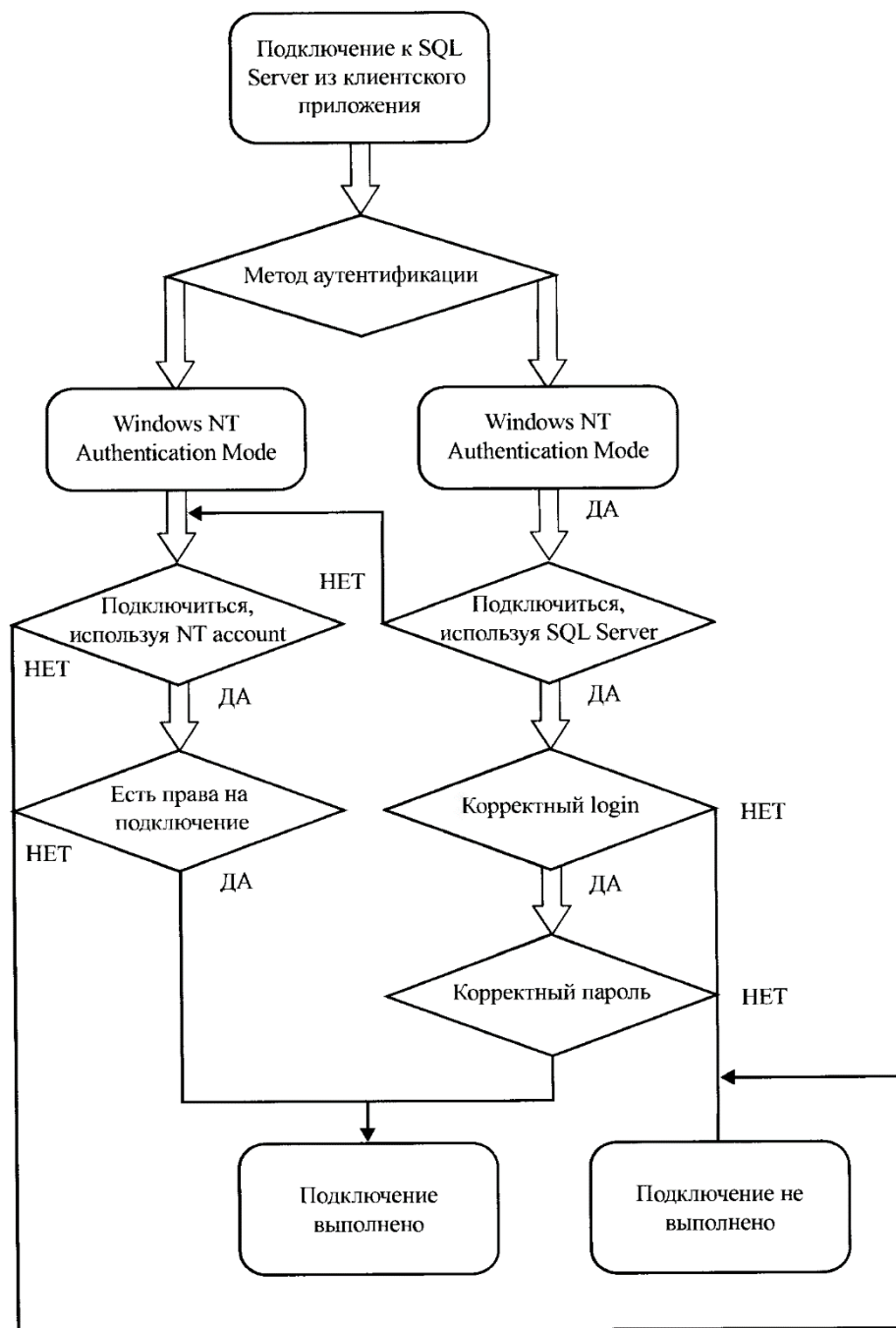


Рисунок 1.13. Алгоритм проверки аутентификации пользователя в MSSQLServer

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.

На пересечении каждого столбца и каждой строки расположен перечень разрешенных операций для данного пользователя над данным объектом. С первого 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 Tab1, 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 следующей 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 персонала (скрытые проверки), аудит, различные процедуры поддержки безопасности, выполняемые вручную или частично автоматизированные.

Оборудование и материалы

Аппаратура. Для выполнения лабораторной работы необходим персональный компьютер со следующими характеристиками: процессор с

тактовой частотой 3000МГц и выше, оперативная память – не менее 4 Гб и более, свободное дисковое пространство – не менее 1000 Мб, устройство для чтения компакт-дисков, монитор типа Super VGA (число цветов – 65535).

Программное обеспечение. Для выполнения лабораторной работы необходима операционная система XP Professional и выше, библиотека Microsoft .NET Framework версии 1.1 или выше, антивирусное ПО.

Указания по технике безопасности

При выполнении лабораторной работы **запрещается:**

- самостоятельно производить ремонт персонального компьютера, а также установку и удаление имеющегося программного обеспечения;
- нарушать общепринятые правила техники безопасности при работе с электрооборудованием, в частности, касаться электрических розеток металлическими предметами и т.д.;
- принимать пищу, напитки и сорить на рабочем месте пользователя персонального компьютера.

В случае неисправности персонального компьютера необходимо **немедленно** сообщить об этом обслуживающему персоналу лаборатории (системному администратору, оператору).

Практическое задание

Разработать проект системы защиты базы данных в соответствии с закрепленным предприятием.

Содержание отчета

1. Титульная страница отчета.
2. Цель лабораторной работы.
3. Ответы на контрольные вопросы.
4. Описание выполненной работы.
5. Вывод.

Контрольные вопросы

1. Назовите основные компоненты подсистемы защиты базы данных.
2. Какие наиболее общие подходы к вопросу обеспечения безопасности данных поддерживаются в современных СУБД?
3. Перечислите наиболее известные современные СУБД.
4. Опишите алгоритм проверки аутентификации пользователя в MSSQLServer.
5. Для чего используется механизм разграничения доступа на уровне СУБД.

Список литературы

1. Сычев Ю. Н., Основы информационной безопасности. Учебно-практическое пособие - М.: Евразийский открытый институт, 2010. - 328 с.
http://old.biblioclub.ru/90790_Osnovy_informatsionnoi_bezopasnosti_Uchebno_prakticheskoe_posobie.html
2. 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.
http://old.biblioclub.ru/86475_Zaschita_kompyuternoi_informatsii_Effektivnye_metody_i_sredstva.html
3. 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.
http://old.biblioclub.ru/93349_Razrabotka_sistemy_tekhnicheskoi_zaschity_informatsii_uchebnoe_posobie.html

Лабораторная работа 7.

Особенности эксплуатации КСИБ на объекте защиты

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:

1. 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.

2. 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 централизованно.

Ниже приведены основные рекомендации, позволяющие снизить вероятность эксплуатации кабельной системы компьютерной сети предприятия злоумышленником.

1. 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.

2. Для подключения критически важных для предприятия серверов используют два кабельных сегмента – основной и резервный.

3. Прокладка сетевого кабеля осуществляется в скрытой проводке, либо в закрываемых кабель-каналах с возможностью опечатывания не срываемыми наклейками – «стикерами».

4. Кабельные сегменты, используемые для подключения всех узлов компьютерной сети, должны быть сконцентрированы на одной коммутационной панели.

5. В начальной конфигурации топологии физических связей должно быть исключено совместное использование среды передачи любой парой узлов сети. Исключение составляет связь с «узел-коммутатор».

6. Управление конфигурацией физических связей между узлами осуществляется только на коммутационной панели.

7. 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.

1. 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.

2. Прокладка высокочастотного кабеля должна быть выполнена скрытым способом либо в коробах с последующим опечатыванием коробов «стикерами».

3. Длина высокочастотного кабельного сегмента должна быть минимальной.

4. Доступ в помещения с радиомодемами, радиомостами и станциями, оснащенными радиосетевыми адаптерами должен строго контролироваться службой безопасности предприятия.

5. Администратор сети должен детально документировать процедуры настройки радиомодемов, радиомостов и станций, оснащенных радиосетевыми адаптерами.

6. Администратор сети должен регулярно менять реквизиты авторизации для удаленного управления этими устройствами.

7. Администратор сети должен выделить отдельный адресный пул для администрирования этих устройств по сети.

8. Администратор сети должен отключить неиспользуемые функции радиомодемов, радиомостов и станций, оснащенных радиосетевыми адаптерами.

9. Администратор должен активировать функции радиомодема или радиомоста обеспечивающие «туннелирование» и криптографическую защиту передаваемых и принимаемых сообщений.

10. 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 разделяться 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 (X), заблаговременно определяет аппаратный и сетевой адреса атакуемых узлов. Затем начинает непрерывно отправлять в адрес узла (A) ложные ответы с указанием сетевого адреса узла (B) и аппаратного адреса своего узла (X). Получая ложные ответы узел (A) перестраивает свою таблицу разрешения сетевых адресов и с этого момента все кадры, отправляемые им в адрес узла (B) 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 (B). Если злоумышленнику необходимо организовать прослушивание трафика между узлами (A) и (B) 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.

1. Администратор службы безопасности должен вести инвентаризационную ведомость соответствия аппаратных и сетевых адресов всех узлов сети предприятия.

2. 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.

3. 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.

4. 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.

5. Администратор сети должен регулярно контролировать соответствие конфигураций коммутаторов разработанной политике защиты.

6. Администратор сети должен вести мониторинг сетевой активности пользователей с целью выявления источников аномально высокого количества широковещательных запросов.

7. Служба безопасности должна контролировать регулярность смены реквизитов авторизации администратора в подсистемах управления коммутаторами.

8. 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 2^n , 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.

Оборудование и материалы

Аппаратура. Для выполнения лабораторной работы необходим персональный компьютер со следующими характеристиками: процессор с тактовой частотой 3000МГц и выше, оперативная память – не менее 4 Гб и более, свободное дисковое пространство – не менее 1000 Мб, устройство для чтения компакт-дисков, монитор типа Super VGA (число цветов – 65535).

Программное обеспечение. Для выполнения лабораторной работы необходима операционная система XP Professional и выше, библиотека Microsoft .NET Framework версии 1.1 или выше, антивирусное ПО.

Указания по технике безопасности

При выполнении лабораторной работы **запрещается:**

- самостоятельно производить ремонт персонального компьютера, а также установку и удаление имеющегося программного обеспечения;
- нарушать общепринятые правила техники безопасности при работе с электрооборудованием, в частности, касаться электрических розеток металлическими предметами и т.д.;

– принимать пищу, напитки и сорить на рабочем месте пользователя персонального компьютера.

В случае неисправности персонального компьютера необходимо **немедленно** сообщить об этом обслуживающему персоналу лаборатории (системному администратору, оператору).

Практическое задание

Разработайте проект организации защищенной телекоммуникационной инфраструктуры в соответствии с закрепленным предприятием.

Содержание отчета

1. Титульная страница отчета.
2. Цель лабораторной работы.
3. Ответы на контрольные вопросы.
4. Описание выполненной работы.
5. Вывод.

Контрольные вопросы

1. Что называется телекоммуникационной инфраструктурой предприятия?
2. Назовите основные уровни модели OSI, используемые для защиты телекоммуникационной инфраструктуры.
3. Назовите основные компоненты защищенной телекоммуникационной инфраструктуры.
4. Перечислите основные методы защиты телекоммуникационной инфраструктуры на канальном уровне.
5. Перечислите основные методы защиты телекоммуникационной инфраструктуры на сетевом уровне.

Список литературы

1. 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.

http://old.biblioclub.ru/93275_Metody_i_sredstva_inzhenerno_tekhnicheskoi_zaschity_informatsii_uchebnoe_posobie.html

2. 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.)

Лабораторная работа 8.

Организационно-функциональные задачи службы безопасности

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).

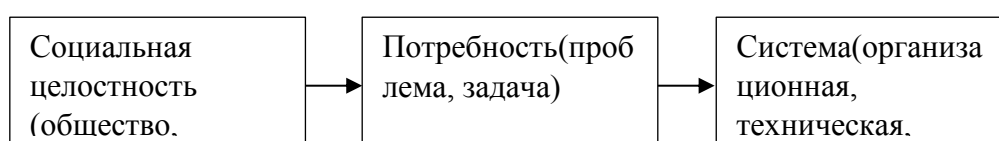


Рисунок 30. Общественная потребность – основа потребления систем

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.

В связи с развитием системного анализа как основного инструментария о 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 удастся, 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.

В 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:

1. Обеспечение заданного уровня достижения цели при минимальном уровне затрат;

2. 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:

1. Обеспечение разделения труда, выражающееся в конкретизации функциональных обязанностей руководителей и специалистов органов управления;

2. 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;

3. 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;

4. Обеспечение психологических совместимостей руководителей и специалистов органов управления со средствами автоматизации;

5. Повышение исполнительской дисциплины работников органов управления.

Главным направлением построения технологии организационного управления, удовлетворяющим перечисленным выше требованиям, является разработка технологий, на индустриальной основе в широком применении вычислительной техники и автоматизации технологических процессов управления.

Чтобы разработать эффективную технологию управления, необходимо решить следующие проблемы:

1. Разработать, утвердить и внедрить стандартные элементы технологии управления;

2. Разработать и внедрить стандартные и методы решения задач всех классов;

3. Максимальная формализация решения всех задач, объективно возникающих в процессе функционирования системы управления;

4. Разработать эффективные средства, методы и способы обеспечения безопасности информации, хранимой и обрабатываемой с использованием ВТ;

5. Разработать нормативно-методические документы, регламентирующие взаимодействие работников органов управления между собой и со средствами автоматизации;

6. 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:

1. Однозначность определения функционального назначения объекта, процесса или явления;

2. Четкость и однозначность общей архитектуры объекта процесса или явления;

3. Простота внутренней организации объекта, процесса или явления в целом, его составных частей и взаимосвязи между ними;

4. Стандартность и унифицированность внутренней структуры элементов их составляющих частей и взаимосвязей между ними;

5. Простота изучения структур и содержания элементов любой их совокупности и взаимосвязей между элементами;

6. Модульность, т. е. автономная организация элементов, позволяющая стандартными способами объединять элементы в сложные структуры, а также заменять любые элементы или совокупность этих элементов;

7. Гибкость, т. е. возможность расширения и реорганизации элементов и их частей без изменения или несущественными изменениями других элементов;

8. 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:

1. Определение совокупности процедур собственно управления, подлежащих осуществлению в соответствующем интервале времени;
2. 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.

В 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 изменившимся 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).



Рисунок 31. Структура процесса управления

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.

Из рис. 32 видно, что планирование является первым 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.

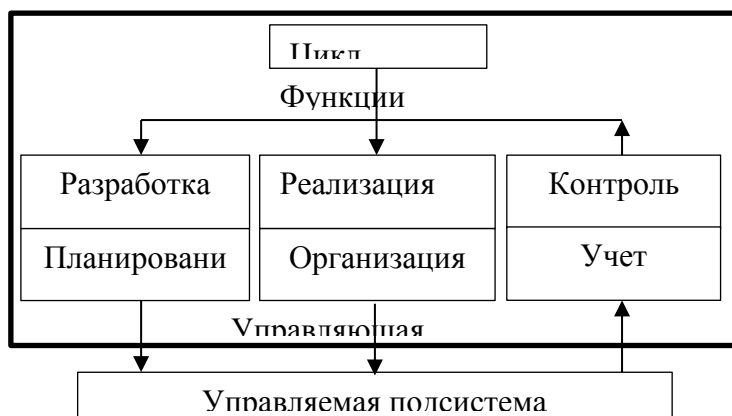


Рисунок 32. Схема связи и взаимодействия функций управления

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 к 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;
- при необходимости может предусматриваться изменение 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:

- 1) директивность, т. е. обязательный характер планов;
- 2) преемственность – сочетание и взаимосвязь перспективного и текущего планирования: использование положительного опыта работы, учет допущенных недостатков и просчетов;
- 3) 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;
- 4) гибкость – наличие возможностей маневра имеющимися силами и средствами в ходе выполнения плана, а также корректировка плана в случае изменения обстановки;
- 5) проблемность – нацеленность мероприятий на решение значимых вопросов, сосредоточение усилий работников на основных направлениях их деятельности, недопущение распыленности в использовании сил и средств;
- 6) 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;

7) 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.

1. *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.

2. *Синтез.* В этом случае сначала составляют планы на низшем уровне, которые затем, последовательно обобщенные, синтезируют в соответствии и иерархической структурой.

3. *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:

1. Способствует ли данное мероприятие достижению поставленных задач, замыслу?
2. Является ли оно правомерным, не противоречит ли законам, нормативным актам?
3. 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 базируются на результатах проделанной работы по выполнению планов за предыдущий период и согласовываются с планами на смежных направлениях деятельности.

В начальной стадии планирования руководитель всесторонне 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:

- 1) организационно-методическая работа;
- 2) контрольно-проверочная работа;
- 3) профилактическая работа;
- 4) работа с кадрами.

В 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.

В 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.

В 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.

7. 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;

2. Анализ сравнения фактического положения с заданным режимом, обстановкой и оценка характера допущенных отклонений и недоработок;

3. 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:

1. Определение обоснованности и практической целесообразности проводимых мероприятий по ЗИ;

2. 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:

1) Проверку выполнения сотрудниками требований по обеспечению сохранности КТ. Такая проверка может проводиться в течение рабочего дня руководителем предприятия, его заместителем, исполнительными директорами, начальниками объектов;

2) 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;

3) Проверку выполнения сотрудниками правил работы с конфиденциальными документами (правила хранения, размножения и копирования) проводит заместителем руководителя в любое время;

4) 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.

Оборудование и материалы

Аппаратура. Для выполнения лабораторной работы необходим персональный компьютер со следующими характеристиками: процессор с тактовой частотой 3000МГц и выше, оперативная память – не менее 4 Гб и более, свободное дисковое пространство – не менее 1000 Мб, устройство для чтения компакт-дисков, монитор типа Super VGA (число цветов – 65535).

Программное обеспечение. Для выполнения лабораторной работы необходима операционная система XP Professional и выше, библиотека Microsoft .NET Framework версии 1.1 или выше, антивирусное ПО.

Указания по технике безопасности

При выполнении лабораторной работы **запрещается:**

- самостоятельно производить ремонт персонального компьютера, а также установку и удаление имеющегося программного обеспечения;
- нарушать общепринятые правила техники безопасности при работе с электрооборудованием, в частности, касаться электрических розеток металлическими предметами и т.д.;

– принимать пищу, напитки и сорить на рабочем месте пользователя персонального компьютера.

В случае неисправности персонального компьютера необходимо **немедленно** сообщить об этом обслуживающему персоналу лаборатории (системному администратору, оператору).

Практическое задание

Разработайте проект организации защиты управления информационной безопасностью инфраструктуры в соответствии с закрепленным предприятием.

Содержание отчета

1. Титульная страница отчета.
2. Цель лабораторной работы.
3. Ответы на контрольные вопросы.
4. Описание выполненной работы.
5. Вывод.

Контрольные вопросы

1. Что называется системой управления информационной безопасностью?
2. Какие стадии включает в себя процесс контроля целостности системы защиты информации?
3. Назовите основные компоненты системы управления информационной безопасностью.
4. Перечислите основные методы защиты систем управления информационной безопасностью.

Список литературы

1. Сычев Ю. Н., Основы информационной безопасности. Учебно-практическое пособие - М.: Евразийский открытый институт, 2010. - 328 с. http://old.biblioclub.ru/90790_Osnovy_informatsionnoi_bezopasnosti_Uчебno_pракticheskoe_posobie.html
2. 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.

http://old.biblioclub.ru/86475_Zaschita_kompyuternoi_informatsii_Effektivnye_metody_i_sredstva.html

3. 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.
http://old.biblioclub.ru/93349_Razrabotka_sistemy_tekhnicheskoi_zaschity_informatsii_uchebnoe_posobie.html

Лабораторная работа 9.

Управление комплексной системой 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) $S = \{S_1, S_2, \dots, S_i, \dots, S_n\}$ и объектов доступа (например, объектов файловой системы) $O = \{O_1, O_2, \dots, O, \dots, O_n\}$.

2) 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 S_i , а столбец – объекту O_j . На пересечении строки и столбца указаны права доступа r_v . Соответствующего субъекта к данному объекту.

3) Тестирование фактического наличия права r_k у субъекта S_j по отношению к объекту O_j (тестирование настроек СЗИ от НСД).

4) Сравнение фактических прав доступа 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:

1) Настройка механизма очистки внешней памяти тестируемого СЗИ от НСД в соответствии с информацией, приведенной в эксплуатационной документации.

2) Создание тестовой последовательности символов на внешнем накопителе ЭВМ, на которой установлено тестируемое СЗИ от НСД.

3) Определение сектора накопителя, в котором располагается тестовая последовательность символов: данный сектор определяется путем поиска тестовой последовательности на накопителе с использованием специализированного программного обеспечения (ПО).

4) Удаление созданного действием 2 файла путем применения штатных средств гарантированного удаления информации СЗИ от НСД.

5) Выполнение анализа сектора внешнего накопителя, определенного действием 3, на предмет наличия в нем созданной ранее последовательности символов (выполняется с помощью специализированного программного обеспечения).

6) 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).

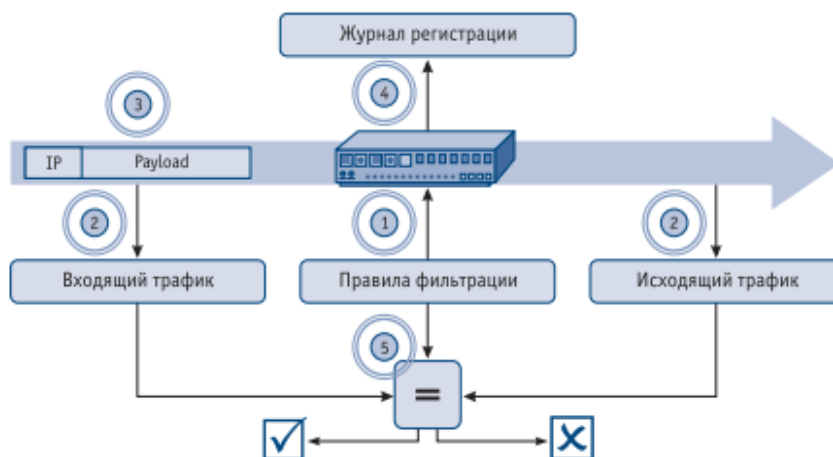


Рисунок 2. Порядок тестирования функций МЭ

1) Настройка правил фильтрации МЭ в соответствии с проверяемым требованием РД [2].

2) Запуск ПО перехвата и анализа сетевых пакетов во внутреннем и внешнем сегментах сети.

3) Генерация сетевых пакетов из внутренней сети во внешнюю (или наоборот), прохождение которых разрешается (запрещается) в соответствии с правилами фильтрации межсетевого экрана.

4) Завершение перехвата сетевых пакетов, экспорт журнала регистрации разрешенных и запрещенных пакетов МЭ.

5) 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 Гостехкомиссии. 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 очистки внешней 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 ресурсах сети;

- локальный аудит паролей учетных записей ОС.

ПК «Сканер-ВС» обладает рядом заметных достоинств:

1) 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.

2) 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

3) поиск, установку и настройку ПО, применяемого при проведении испытаний, в том числе и операционной системы, под которой функционирует тестовое ПО.

4) Сертификаты соответствия. ПК «Сканер-ВС» является сертифицированным в системах сертификации СЗИ ФСТЭК России Минобороны России средством контроля эффективности применения СЗИ.

Оборудование и материалы

Аппаратура. Для выполнения лабораторной работы необходим персональный компьютер со следующими характеристиками: процессор с тактовой частотой 3000МГц и выше, оперативная память – не менее 4 Гб и более, свободное дисковое пространство – не менее 1000 Мб, устройство для чтения компакт-дисков, монитор типа Super VGA (число цветов – 65535).

Программное обеспечение. Для выполнения лабораторной работы необходима операционная система XP Professional и выше, библиотека Microsoft .NET Framework версии 1.1 или выше, антивирусное ПО.

Указания по технике безопасности

При выполнении лабораторной работы **запрещается:**

- самостоятельно производить ремонт персонального компьютера, а также установку и удаление имеющегося программного обеспечения;
- нарушать общепринятые правила техники безопасности при работе с электрооборудованием, в частности, касаться электрических розеток металлическими предметами и т.д.;
- принимать пищу, напитки и сорить на рабочем месте пользователя персонального компьютера.

В случае неисправности персонального компьютера необходимо **немедленно** сообщить об этом обслуживающему персоналу лаборатории (системному администратору, оператору).

Практическое задание

В соответствии с рассмотренными методиками разработайте план мероприятий по испытанию системы защиты объекта информатизации.

Контрольные вопросы

1. Назовите порядок проведения испытаний системы защиты.
2. Назовите порядок разработки методики испытаний.

3. Какой нормативный документ устанавливает 7 классов защищенности средств защиты информации?

4. Назовите порядок тестирования функций МЭ.

5. Каким рядом заметных достоинств обладает программный комплекс «Сканер-ВС»?

Список литературы

1. 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.

2. 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.
http://old.biblioclub.ru/93349_Razrabotka_sistemy_tekhnicheskoi_zaschity_informat_sii_uchebnoe_posobie.html

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

Методические указания

по организации и проведению самостоятельной работы
по дисциплине

«Информационная безопасность»

для студентов направления подготовки

09.03.02 «Информационные системы и технологии»

направленность (профиль)

**«Прикладное программирование в интеллектуальных информационных
системах»**

Ставрополь, 2025

1. Общие положения

Самостоятельная работа – планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Самостоятельная работа студентов (СРС) в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.

К основным видам самостоятельной работы студентов относятся:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- написание докладов;
- подготовка к семинарам, практическим и лабораторным работам, их оформление;
- составление аннотированного списка статей из соответствующих журналов по отраслям знаний (педагогических, психологических, методических и др.);
- выполнение учебно-исследовательских работ, проектная деятельность;
- подготовка практических разработок и рекомендаций по решению проблемной ситуации;
- выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и т.д.;
- компьютерный текущий самоконтроль и контроль успеваемости на базе электронных обучающих и аттестующих тестов;
- выполнение курсовых работ (проектов) в рамках дисциплин;
- выполнение выпускной квалификационной работы и др.

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных качеств студентов и условий учебной деятельности.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

- подготовительный (определение целей, составление программы, подготовка методического обеспечения, подготовка оборудования);
- основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);
- заключительный (оценка значимости и анализ результатов, их систематизация, оценка эффективности программы и приемов работы, выводы о направлениях оптимизации труда).

Самостоятельная работа по дисциплине «Информационная безопасность» направлена на формирование следующих **компетенций**:

Код, формулировка компетенции	Код, формулировка индикатора
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с	ИД-1 _{ОПК-3} Использует принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с

применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	учетом основных требований информационной безопасности.
	ИД-2 _{ОПК-3} Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
	ИД-3 _{ОПК-3} Осуществляет подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.

2. Цель и задачи самостоятельной работы

Ведущая цель организации и осуществления СРС совпадает с целью обучения студента – формирование набора общенаучных, профессиональных и специальных компетенций будущего бакалавра по соответствующему направлению подготовки

При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности. Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;
- формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений;
- использование материала, собранного и полученного в ходе самостоятельных занятий на семинарах, на практических и лабораторных занятиях, при написании курсовых и выпускной квалификационной работ, для эффективной подготовки к итоговым зачетам и экзаменам.

3. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе (акад.)		
			СРС	Контактная работа с преподавателям	Всего
6 семестр					
ОПК-3	Самостоятельное изучение литературы и источников	Собеседование	4	2	6
ОПК-3	Подготовка лабораторным занятиям	Защита ЛР	70	4	74
Итого за 6 семестр			74	6	80
Итого			74	6	80

4. Порядок выполнения самостоятельной работы студентом

4.1. Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют **четыре основные установки в чтении научного текста:**

информационно-поисковый (задача – найти, выделить искомую информацию)

усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения излагаемые автором, так и всю логику его рассуждений)

аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Методические рекомендации по составлению конспекта:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта;

2. Выделите главное, составьте план;

3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора;

4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.

5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

4.2. Методические рекомендации по подготовке к практическим и лабораторным занятиям

Для того чтобы практические и лабораторные занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на практических занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

4.3. Методические рекомендации по самопроверке знаний

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется, провести самопроверку усвоенных знаний, ответив на контрольные вопросы по изученной теме.

В случае необходимости нужно еще раз внимательно разобраться в материале.

Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала - умение решать задачи или пройти тестирование по пройденному материалу. Однако следует помнить, что правильное решение задачи может получиться в результате применения механически заученных формул без понимания сущности теоретических положений.

4.4. Методические рекомендации по написанию научных текстов (докладов, докладов, эссе, научных статей и т.д.)

Перед тем, как приступить к написанию научного текста, важно разобраться, какова истинная цель вашего научного текста - это поможет вам разумно распределить свои силы и время.

Во-первых, сначала нужно определиться с идеей научного текста, а для этого необходимо научиться либо относиться к разным явлениям и фактам несколько критически (своя идея – как иная точка зрения), либо научиться увлекаться какими-то известными идеями, которые нуждаются в доработке (идея – как оптимистическая позиция и направленность на дальнейшее совершенствование уже известного). Во-вторых, научиться организовывать свое время, ведь, как известно, свободное (от всяких глупостей) время –

важнейшее условие настоящего творчества, для него наконец-то появляется время. Иногда именно на организацию такого времени уходит немалая часть сил и талантов.

Писать следует ясно и понятно, стараясь основные положения формулировать четко и недвусмысленно (чтобы и самому понятно было), а также стремясь структурировать свой текст. Каждый раз надо представлять, что ваш текст будет кто-то читать и ему захочется сориентироваться в нем, быстро находить ответы на интересующие вопросы (заодно представьте себя на месте такого человека). Понятно, что работа, написанная «сплошным текстом» (без заголовков, без выделения крупным шрифтом наиболее важным мест и т. п.), у культурного читателя должна вызывать брезгливость и даже жалость к автору (исключения составляют некоторые древние тексты, когда и жанр был иной и к текстам относились иначе, да и самих текстов было гораздо меньше – не то, что в эпоху «информационного взрыва» и соответствующего «информационного мусора»).

Объем текста и различные оформительские требования во многом зависят от принятых в конкретном учебном заведении порядков.

Доклад – это самостоятельное исследование студентом определенной проблемы, комплекса взаимосвязанных вопросов.

Доклад не должна составляться из фрагментов статей, монографий, пособий. Кроме простого изложения фактов и цитат, в доклад е должно проявляться авторское видение проблемы и ее решения.

Рассмотрим основные этапы подготовки
а студентом.

Выполнение доклада начинается с выбора темы.

Затем студент приходит на первую консультацию к руководителю, которая предусматривает:

- обсуждение цели и задач работы, основных моментов избранной темы;
- консультирование по вопросам подбора литературы;
- составление предварительного плана.

Следующим этапом является работа с литературой. Необходимая литература подбирается студентом самостоятельно.

После подбора литературы целесообразно сделать рабочий вариант плана работы. В нем нужно выделить основные вопросы темы и параграфы, раскрывающие их содержание.

Составленный список литературы и предварительный вариант плана уточняются, согласуются на очередной консультации с руководителем.

Затем начинается следующий этап работы – изучение литературы. Только внимательно читая и конспектируя литературу, можно разобраться в основных вопросах темы и подготовиться к самостоятельному (авторскому) изложению содержания доклада. Конспектируя первоисточники, необходимо отразить основную идею автора и его позицию по исследуемому вопросу, выявить проблемы и наметить задачи для дальнейшего изучения данных проблем.

Систематизация и анализ изученной литературы по проблеме исследования позволяют студенту написать работу.

Рабочий вариант текста доклада предоставляется руководителю на проверку. На основе рабочего варианта текста руководитель вместе со студентом обсуждает возможности доработки текста, его оформление. После доработки доклад сдается на кафедру для его оценивания руководителем.

Требования к написанию доклада

Написание 1 доклада является обязательным условием выполнения плана СРС по любой дисциплине профессионального цикла.

Тема доклада может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно, исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласовать с преподавателем.

Доклад должен быть написан научным языком.

Объем доклада должен составлять 20-25 стр.

Структура доклада:

- Введение (не более 3-4 страниц). Во введении необходимо обосновать выбор темы, ее актуальность, очертить область исследования, объект исследования, основные цели и задачи исследования.

- Основная часть состоит из 2-3 разделов. В них раскрывается суть исследуемой проблемы, проводится обзор мировой литературы и источников Интернет по предмету исследования, в котором дается характеристика степени разработанности проблемы и авторская аналитическая оценка основных теоретических подходов к ее решению. Изложение материала не должно ограничиваться лишь описательным подходом к раскрытию выбранной темы. Оно также должно содержать собственное видение рассматриваемой проблемы и изложение собственной точки зрения на возможные пути ее решения.

- Заключение (1-2 страницы). В заключении кратко излагаются достигнутые при изучении проблемы цели, перспективы развития исследуемого вопроса

- Список использованной литературы (не меньше 10 источников), в алфавитном порядке, оформленный в соответствии с принятыми правилами. В список использованной литературы рекомендуется включать работы отечественных и зарубежных авторов, в том числе статьи, опубликованные в научных журналах в течение последних 3-х лет и ссылки на ресурсы сети Интернет.

- Приложение (при необходимости).

Требования к оформлению:

- текст с одной стороны листа;
- шрифт Times New Roman;
- кегль шрифта 14;
- межстрочное расстояние 1,5;
- поля: сверху 2,5 см, снизу – 2,5 см, слева - 3 см, справа 1,5 см;
- доклад должен быть представлен в сброшюрованном виде.

Порядок защиты доклада:

Защита доклада проводится на практических занятиях, после окончания работы студента над ним и исправления всех недочетов, выявленных преподавателем в ходе консультаций. На защиту доклада отводится 5-7 минут времени, в ходе которого студент должен показать свободное владение материалом по заявленной теме. При защите доклада приветствуется использование мультимедиа-презентации.

Оценка доклада

Доклад оценивается по следующим критериям:

- соблюдение требований к его оформлению;
- необходимость и достаточность для раскрытия темы приведенной в тексте доклада информации;
- умение студента свободно излагать основные идеи, отраженные в докладе;
- способность студента понять суть задаваемых преподавателем и сокурсниками вопросов и сформулировать точные ответы на них.

Критерии оценки:

Оценка «отлично» выставляется студенту, если в докладе студент исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует для написания доклада современные научные материалы; анализирует полученную информацию; проявляет самостоятельность при написании доклада.

Оценка «хорошо» выставляется студенту, если качество выполнения доклада достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопросы по теме доклада.

Оценка «удовлетворительно» выставляется студенту, если материал доклада излагается частично, но пробелы не носят существенного характера, студент допускает неточности и ошибки при защите доклада, дает недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении материала.

Оценка «неудовлетворительно» выставляется студенту, если он не подготовил доклад или допустил существенные ошибки. Студент неуверенно излагает материал доклада, не отвечает на вопросы преподавателя.

4.5. Методические рекомендации по выполнению исследовательских проектов

Исследовательская проектная работа – это групповая работа, для выполнения которой необходим выбор и приложение научной методики к поставленной задаче, получение собственного теоретического или экспериментального материала, на основании которого необходимо провести анализ и сделать выводы об исследуемом явлении. Выполнение проекта – это всегда коллективная, творческая практическая работа, предназначенная для получения определенного продукта или научно-технического результата. Такая работа подразумевает четкое, однозначное формирование поставленной задачи, определение сроков выполнения намеченного, определение требований к разрабатываемому объекту.

Выполнение 1 группового проекта является обязательным условием выполнения самостоятельной работы по любой дисциплине профессионального цикла. Тема проектного задания может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно, исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласовать с преподавателем.

Требования по выполнению и оформлению проекта

При выполнении проекта приветствуется работа в группе (2-3 человека). Проект – это исследовательская работа, в ходе которой студенты должны продемонстрировать владение навыками научного исследования, умения проводить анализ, обобщать информацию, делать выводы, предлагать свои решения проблемы, рассматриваемой в проекте.

При подготовке материалов проекта студенты должны продемонстрировать владение современными методами компьютерной обработки данных.

Критерии оценки работы участника проекта.

Для каждого из участников проекта оцениваются:

- профессиональные теоретические знания в соответствующей области;
- умение работать со справочной и научной литературой, осуществлять поиск необходимой информации в Интернет;
- умение работать с техническими средствами;
- умение пользоваться соответствующими выполняемому проекту информационными технологиями;
- умение готовить материалы проекта для презентации: составлять и редактировать тексты, формировать презентацию проекта;
- умение работать в команде;
- умение публично представлять результаты собственной деятельности;
- коммуникабельность, инициативность, творческие способности.

Критерии выставления оценки участникам проекта

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
«Отлично»	Работа выполнена на высоком профессиональном уровне. Представленный материал в основном фактически верен, допускаются негрубые фактические неточности. Студент свободно отвечает на вопросы, связанные с проектом.	Технические средства и информационные технологии освоены и использованы для реализации проекта полностью	Студент проявил инициативу, творческий подход, способность к выполнению сложных заданий, навыки работы в коллективе, организационные способности.	Проект представлен полностью и в срок.
«Хорошо»	Работа выполнена на достаточно высоком профессиональном уровне. Допущено до 4–5 фактических ошибок. Студент отвечает на вопросы, связанные с проектом, но недостаточно полно.	Обнаруживаются некоторые ошибки в использовании соответствующих технических средств и информационных технологий	Студент достаточно полно, но без инициативы и творческих находок выполнил возложенные на него задачи.	Проект представлен достаточно полно и в срок, но с некоторыми недоработками.
«Удовлетворительно»	Уровень недостаточно высок. Допущено до 8 фактических ошибок. Студент может ответить лишь на некоторые из заданных вопросов, связанных с проектом.	Обнаруживает недостаточное владение навыками работы с техническими средствами и соответствующим и информационным и технологиями	Студент выполнил большую часть возложенной на него работы.	Проект сдан со значительным опозданием (более недели) и не полностью
«Неудовлетворительно»	Работа не выполнена или выполнена на низком уровне. Допущено более 8 фактических ошибок. Ответы на связанные с проектом вопросы	Навыков работы с техническими средствами нет, информационные технологии не освоены	Студент практически не работал, не выполнил свои задачи или выполнил лишь отдельные не существенные	Проект не сдан.

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
	обнаруживают непонимание предмета и отсутствие ориентации в материале проекта.		поручения в групповом проекте.	

Студенты должны: защитить проект в режиме презентации, предъявить файлы выполненного проекта, уметь рассказать о технологиях, использованных ими при выполнении проекта, дать оценку работы каждого члена группы (*если проект групповой*).

4.6. Методические рекомендации по подготовке к экзаменам и зачетам

Изучение многих общепрофессиональных и специальных дисциплин завершается экзаменом. Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На экзамене студент демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине.

Экзаменационная сессия - это серия экзаменов, установленных учебным планом. Между экзаменами интервал 3-4 дня. Не следует думать, что 3-4 дня достаточно для успешной подготовки к экзаменам.

В эти 3-4 дня нужно систематизировать уже имеющиеся знания. На консультации перед экзаменом студентов познакомят с основными требованиями, ответят на возникшие у них вопросы. Поэтому посещение консультаций обязательно.

Требования к организации подготовки к экзаменам те же, что и при занятиях в течение семестра, но соблюдаться они должны более строго. Во-первых, очень важно соблюдение режима дня; сон не менее 8 часов в сутки, занятия заканчиваются не позднее, чем за 2-3 часа до сна. Оптимальное время занятий - утренние и дневные часы. В перерывах между занятиями рекомендуются прогулки на свежем воздухе, неустойчивые занятия спортом. Во-вторых, наличие хороших собственных конспектов лекций. Даже в том случае, если была пропущена какая-либо лекция, необходимо во время ее восстановить (переписать ее на кафедре), обдумать, снять возникшие вопросы для того, чтобы запоминание материала было осознанным. В-третьих, при подготовке к экзаменам у студента должен быть хороший учебник или конспект литературы, прочитанной по указанию преподавателя в течение семестра. Здесь можно эффективно использовать листы опорных сигналов.

Вначале следует просмотреть весь материал по сдаваемой дисциплине, отметить для себя трудные вопросы. Обязательно в них разобраться. В заключение еще раз целесообразно повторить основные положения, используя при этом листы опорных сигналов.

Систематическая подготовка к занятиям в течение семестра позволит использовать время экзаменационной сессии для систематизации знаний.

Контроль самостоятельной работы студентов

Контроль самостоятельной работы проводится преподавателем в аудитории.

Предусмотрены следующие виды контроля: собеседование, оценка доклада, оценка презентации, оценка участия в круглом столе, оценка выполнения проекта.

Подробные критерии оценивания компетенций приведены в Фонде оценочных средств для проведения текущей и промежуточной аттестации.

Список литературы для выполнения СРС

Перечень основной литературы:

1. средства инженерно-технической защиты информации : учебное пособие. 2-е изд., стер. - М.: Флинта, 2011. - 187 с.
http://old.biblioclub.ru/93275_Metody_i_sredstva_inzhenerno_tekhnicheskoi_zaschity_informatsii_uchebnoe_posobie.html
2. 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.)
3. Чипига, А. Ф. Информационная безопасность автоматизированных систем : учеб. пособие / А. Ф. Чипига. – М. : Гелиос АРВ, 2010. – 336 с.
4. 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.

Перечень дополнительной литературы:

1. 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.
2. Сергеева Ю. С. Защита информации. Конспект лекций. Учебное пособие. - М.: А-Приор, 2011. - 128 с.
http://old.biblioclub.ru/72670_Zaschita_informatsii_Konspekt_leksii_Uchebnoe_posobie.html
3. Сычев Ю. Н., Основы информационной безопасности. Учебно-практическое пособие - М.: Евразийский открытый институт, 2010. - 328 с.
http://old.biblioclub.ru/90790_Osnovy_informatsionnoi_bezopasnosti_Uchebno_prakticheskoe_posobie.html
4. 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.
http://old.biblioclub.ru/86475_Zaschita_kompyuternoi_informatsii_Effektivnye_metody_i_sredstva.html

Методическая литература:

1. Методические рекомендации для самостоятельной работы студентов по дисциплине «Информационная безопасность»
2. Методические указания к лабораторным работам по дисциплине «Информационная безопасность»

Интернет-ресурсы:

1. <http://el.ncfu.ru/> – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Информационная безопасность».
2. <http://www.un.org> - Сайт ООН Информационно-коммуникационные технологии.
3. <http://www.intuit.ru> – Интернет-Университет Компьютерных технологий.

