

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 «Комплексная система защиты информации на предприятии»
для студентов направления подготовки
10.03.01 «Информационная безопасность»
Направленность (профиль)
«Организация и технологии защиты информации (по отрасли или в сфере
профессиональной деятельности)»

Ставрополь
2026

СОДЕРЖАНИЕ

Тема 1. Сущность и задачи комплексной системы защиты информации на предприятии

Лабораторная работа 1 Подбор технических средств для обеспечения защиты информации

Лабораторная работа 2 Анализ рисков безопасности информации

Тема 2. Принципы организации и этапы разработки комплексной системы защиты информации

Лабораторная работа 3 Разработка моделей объектов защиты

Теоретическая часть

Лабораторная работа 4 Структурирование защищаемой информации

Тема 3. Факторы влияющие на организацию комплексной системы защиты информации

Лабораторная работа 5 Моделирование технических каналов утечки информации

Лабораторная работа 6 Системный анализ информационной безопасности и принятие решения о защите информации правовыми и организационными методами

Тема 4. Определение и нормативное закрепление состава защищаемой информации

Лабораторная работа 7 Системный анализ информационной безопасности и принятие решения о защите информации от случайных угроз Лабораторная работа 8

Системный анализ информационной безопасности

и принятие решения по защите информации от традиционного шпионажа и диверсий

Тема 5. Разработка модели комплексной системы защиты информации

Лабораторная работа 9 Системный анализ информационной безопасности

и принятие решения по ее защите от электромагнитных излучений и наводок

Лабораторная работа 10 Системный анализ информационной безопасности

и принятие решения по ее защите от несанкционированного изменения структур

Тема 6. Технологическое и организационное построение комплексной системы защиты информации

Лабораторная работа 11 Системный анализ информационной безопасности и принятие решения по ее защите от несанкционированного доступа в компьютерную сеть .

Лабораторная работа № 12 Системный анализ информационной

безопасности и принятие решения по ее защите криптографическими методами.

Тема 7. Назначение, структура и содержание управления комплексной системы защиты информации

Лабораторная работа 13 Системный анализ информационной безопасности и принятие решения по ее защите от компьютерных вирусов

Лабораторная работа 14 Системный анализ информационной безопасности и принятие решения по ее защите в распределенных компьютерных сетях ..

Тема 8. Общая характеристика подходов к оценке эффективности комплексной системы защиты информации

Лабораторная работа 15 Системный анализ информационной безопасности

и принятие решения по инженерно-технической защите охраняемого объекта

Лабораторная работа 16 Системный анализ информационной безопасности и принятие решения по ее защите с использованием комплексной системы защиты информации

.....

ВВЕДЕНИЕ

■ 1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины является формирование профессиональных компетенций в области комплексной системы защиты информации, методики и технологии ее организации на предприятии, принципов и содержания управления системой, методов обеспечения ее надежности.

Задачи освоения дисциплины...

- дать основы сущности, целей и задач комплексной системы защиты информации, принципов и этапов ее разработки;
- освоить технологии установления состава защищаемой информации и объектов защиты, получить необходимые знания по методам оценки уязвимости защищаемой информации;
- научиться определять параметры и структуру комплексной системы защиты информации, проведению мероприятий по обеспечению функционирования комплексной системы защиты информации;
- познакомить со структурой и методами управления комплексной системой защиты информации, подходами к определению показателей эффективности и методиками ее оценки.

■ 2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
-------------------------------	------------------------------	---

ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ИД-1 Использует методологический базис теории защиты информации, используемый при разработке формировании политики информационной безопасности ИД-2 Осуществляет организацию и поддерживает выполнение комплекса мер по обеспечению информационной безопасности на объекте защиты в качестве технического специалиста ИД-3 Управляет процессом выполнения комплекса мер по обеспечению	ИД-1 Уверенно использует методологический базис теории защиты информации, используемый при разработке формировании политики информационной безопасности ИД-2 Уверенно осуществляет организацию и поддерживает выполнение комплекса мер по обеспечению информационной безопасности на объекте защиты в качестве технического специалиста ИД-3
--	---	---

	информационной безопасности реализации на объекте защиты в качестве технического специалиста	Способен управлять процессом выполнения комплекса мер по обеспечению информационной безопасности реализации на объекте защиты в качестве технического специалиста
--	---	--

ОПК-2.2 Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы	ИД-1 Демонстрирует понимание оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих, а также устойчивости к деструктивным воздействиям на информационные ресурсы предприятия ИД-2 Демонстрирует способность формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих	ИД-1 Уверенно демонстрирует понимание оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих, а также устойчивости к деструктивным воздействиям на информационные ресурсы предприятия ИД-2 Уверенно демонстрирует способность формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих
ОПК-2.3 Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и		

стандартов безопасности	лационной	ИД-3 Демонстрирует знания комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	ИД-3 Уверенно демонстрирует знания комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности
		ИД-4 Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	ИД-4 Демонстрирует способность разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности

ОПК-2.4 Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами	ИД-3 Демонстрирует процедур защищенности информатизации нормативных док определяющих содержание	ИД-3 Демонстрирует уверенные знания процедур аудита защищенности объекта информатизации и нормативных документов, определяющих его содержание
	ИД-4 Осуществляет защищенности информатизации соответствии нормативными документами знания аудита объекта и ументов, его аудит объекта в с	ИД-4 Способен осуществлять аудит защищенности объекта информатизации в соответствии с нормативными документами

ПЛАНЫ ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Тема 1. Сущность и задачи комплексной системы защиты информации на предприятии

Лабораторная работа 1

Название работы: Подбор технических средств для обеспечения защиты информации

Цель работы:

- изучить теоретический материал;
- отработать навыки по организации комплексной защиты объекта. Время 1,5 часа

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Теоретическая часть

Каждое крупное предприятие требует детального изучения возможных угроз. В каждом конкретном случае требуется свое решение. В то же время есть много общего.

Любое предприятие своего рода крепость. В качестве вступления обратим внимание на некоторые важные моменты.

Периметр предприятия - это комплекс инженерных сооружений (колючая проволока, высокий забор) , полосы отторжения (как раз для случая перекидывания через забор) и инженерных систем (периметральная система, система видеонаблюдения). Все это системы достаточно сложные в настройке и обслуживании. Их установку лучше доверять профессионалам. Это позволит избавиться от ложных срабатываний из-за снега, дождя, мелких животных и птиц, изменения времени суток, температурных условий и пр. Сегодня существует довольно широкий выбор видеосистем, которые могут использоваться для подобных задач. Выбор периметральной системы во многом зависит от необходимой степени защищенности, размера периметра, климата местности.

Ворота или проходные. Их оснащение - очень ответственная задача, степень сложности которой в первую очередь зависит от количества людей ежедневно проходящих через проходные и интенсивности потока в часы

"пик". Здесь следует обратить внимание на технические средства (турникеты, шлюзы), некоторые из которых качественно выполняют свои задачи лишь при небольшом количестве пользователей, а на больших предприятиях часто выходят из строя.

Второй важный момент - характеристики контроллера, обслуживающего турникет. Некоторые типы контроллеров имеют небольшой объем энергонезависимой памяти, а при работе с большим числом людей используют память компьютера. Мы не рекомендовали бы использовать такие контроллеры - потеря связи с компьютером вследствие банального нарушения целостности кабеля приведет к блокированию деятельности проходной, скоплению людей, нарушению трудовой деятельности и другим неприятным последствиям.

Третий важный момент на проходной - тип используемого кодоносителя. Кодоносители отличаются не только стоимостью, но и степенью защищенности. К примеру, штрихкодовые кодоносители подделываются обычным копировальным аппаратом. Некоторые другие виды - более сложными способами, но также вполне возможными. Скорее всего наиболее высокая степень защищенности достигается при использовании биометрических систем (по радужной оболочке глаза, по отпечатку пальца, по руке), но они пока не получили высокого распространения из-за высокой цены и, самое главное, сложности хранения и обработки кодов пользователей (коды очень длинные и при большом количестве пользователей сильно "тормозят" систему.) Поэтому выбор кодоносителя - также задача, требующая осмысления.

Четвертое, что важно - сама программа для проходной. Это то место, с которого мы начнем рассказ про автоматизированные рабочие места, сокращенно АРМ. Современная система безопасности для крупного объекта - это интегрированная система, объединяющая различные службы и включающая в себя разные системы. Если система состоит из нескольких компьютеров, каждый из них получает "специализацию", а к ней - специализированный интерфейс. Интерфейс позволяет постовому выполнять вверенные задачи с максимальной эффективностью. Вернемся к АРМ для проходной - разумеется, на экран должна выводиться большая фотография проходящего. Дополнительно может выводиться и изображение с видеокамеры, фиксирующей человека. Перед тем, как

перейти к другим частям системы безопасности крупного объекта, стоит остановиться на еще одном специальном устройстве для проходной - картоприемнике. Это специальное устройство, которое разблокирует турникет на выход при попадании в него карты доступа гостя, что значительно облегчает контроль за изъятием карты.

АРМ "Бюро пропусков" - важнейший элемент системы безопасности. В системах, устанавливаемых нашей компанией, АРМ позволяет осуществлять учет разрешений на выдачу пропуска в электронном виде (распоряжение может быть направлено служебной запиской или письмом по электронной почте). Различные варианты системы для Бюро Пропусков позволяют фотографировать документы, самих посетителей, изготавливать бумажные пропуска или в виде пластиковых карточек. При этом в систему может быть заложен срок действия пропуска, данные о частоте посещений и др. информация, которая может потребоваться в дальнейшем.

АРМ "КПП". Во многих случаях АРМ "КПП" сопряжен с АРМ "Проходная". Но наиболее "продвинутые" АРМ "КПП" фиксируют номер подъехавшего к выезду автомобиля, сравнивает вес автомобиля с весом при загрузке. Специальный модуль определяет номер и сравнивает его с системой внутрифирменного документооборота, с целью определить санкционированность выезда. Дополнительно может вестись видеозапись въезда-выезда, досмотра автомобиля и фотозапись. Кроме этого, некоторые проходные оснащаются специальными считывателями, позволяющими идентифицировать автомобиль и сидящего в нем водителя. Разумеется, число функций в значительной степени влияет на интерфейс АРМ "КПП".

АРМ "Контрольный терминал". Таких АРМ может быть сколь угодно много. Каждый из них служит для контроля определенного участка (здания, этажа, группы зданий) и всех входящих систем (хотя иногда, в связи с разделением обязанностей различных служб предприятия разделяют контрольный терминал противопожарных систем, контрольный терминал видеосистем и контрольный терминал системы контроля доступа и охранной системы). Этот вид терминала не имеет строгой специализации и в большинстве случаев включает "отображение на плане", "мониторинг событий", "архив событий".

АРМ "Автопарковка" - парковки большинства крупных предприятий ограничены. Конечно для определенных сотрудников могут быть выделены

стационарные места. Для указания места автопарковки остальным служит АРМ "Автопарковка".

АРМ "Столовая" - условное название. Некоторые виды кодоносителей позволяют использовать их как кошелек. Этот вид АРМ позволяет "снимать" деньги с кодоносителя, например, при оплате в столовой (спортзале и пр.)

АРМ "Видеонаблюдение" На большинстве предприятий система видео наблюдения отделена от других систем. Современные системы - это приборы, которые могут сохранять информацию в цифровом виде, передавать ее по сети, активизироваться только при наличии движения.

Современная комплексная система безопасности объекта не ограничивается только функциями безопасности. Она глубоко интегрируется с системой автоматизации (например "опустить лифты и открыть двери при пожаре"), системой защиты информации (например, включение персонального компьютера только при наличии человека в помещении), документооборота (например предоставление данных о посещениях-опозданиях в отдел кадров в установленном законодательством виде).

Практическая часть

Комбинированная система охраны офиса (на приборах "Сигнал-20П"): 15 кабинетов, 3 охранных шлейфа на каждый - дверь, окно, объем и один пожарный (рис. 1.1).

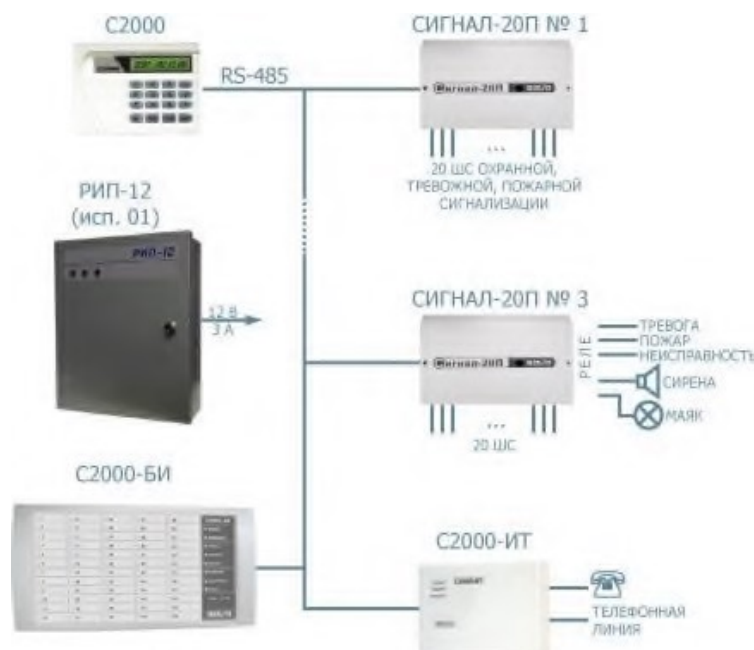


Рисунок 1.1

Система строится на приборах Сигнал-20П, управление и отображение информации на ПКУ С2000. В шлейфы сигнализации приборов можно включать как контактные, так и токопотребляющие охранные и пожарные извещатели. К релейным и транзисторным выходам приборов подключаются выходы "Тревога", "Пожар", "Неисправность" для их передачи на пульт централизованного наблюдения (ПЦН), а также звуковые и световые оповещатели. Возможна установка блока индикации С2000-БИ для оперативной оценки состояния охранной и пожарной сигнализации всех кабинетов. При использовании информатора телефонного С2000-ИТ возможна передача речевых сообщений на телефоны ответственных лиц и передача извещений на ПЦН с установленным на нем программноаппаратным комплексом автоматизации деятельности ПЦО "Эгида". Для взятия кабинетов под охрану и снятия их с охраны используется пульт С2000, на индикаторе которого отображаются все сообщения, приходящие от приборов. Все сообщения хранятся в буфере С2000 емкостью 255 сообщений. Для питания приборов С2000, Сигнал-20П, С2000-ИТ, С2000БИ необходимо применить источник бесперебойного питания РИП-12 .

Задание:

1. Проанализировать пример.

2. Внедрить в данную систему пожарные датчики.
3. Рассчитать примерную стоимость оборудования по прайсам в приложении к лабораторным работам.

Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

Интернет-ресурсы: 1-3

Программное обеспечение: 1-2

Лабораторная работа 2

Название работы: Анализ рисков безопасности информации

Цели:

1. Получить навыки оценки рисков безопасности информационной системы предприятия.
2. Получить практический опыт подбора критериев информационной безопасности системы
3. Закрепить теоретические навыки, полученные на лекциях

Время 1,5 часа

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Введение

При построении комплексных систем защиты информации зачастую трудно определить уровень различных угроз безопасности. Это может привести к неадекватным мерам по их нейтрализации. Для избежания подобных ситуаций необходима количественная оценка степени влияния угроз безопасности информации на информационную систему.

Целью анализа рисков является количественная оценка угроз и уязвимостей, позволяющая определить комплекс контрмер, обеспечивающий достаточный уровень защищенности информационной системы.

Теоретическая часть

При проведении оценки рисков необходимо иметь чёткое представление таких понятий, *угроза* информационной безопасности и *уязвимость* информационной системы или системы защиты информации.

Угроза – совокупность условий и факторов, которые могут стать причиной снижения заданного уровня безопасности информации.

Уязвимость – слабость в системе защиты, которая делает возможным реализацию угрозы.

Риск нарушения ИБ – возможность реализации угрозы.

Величину риска можно определить, исходя из следующей формулы:

$$R(\oplus)C = P_y, \quad (2.1)$$

где: P – величина риска,

C – стоимость информационного ресурса,

P_y – вероятность реализации угрозы.

Стоимость информационного ресурса – это количественная величина, характеризующая степень влияния данного ресурса на информационную систему. Его можно определить как уровень потерь, понесённых владельцами ресурса или информационной системой при его утрате или разглашении. В зависимости от реальных условий, стоимость может быть выражена либо в деньгах, либо условных единицах.

Вероятность реализации угрозы зависит от множества факторов.

Основными из них будут:

- наличие самой угрозы;
- наличие и вероятность реализации уязвимостей системы; – привлекательности уязвимости.

В рамках проведения данной лабораторной работы условимся не учитывать привлекательность той или иной уязвимости. Поскольку наличие угрозы может зависеть от субъективных факторов, например, желания злоумышленника реализовать угрозу, условимся не учитывать и этот фактор. Таким образом, примем вероятность реализации угрозы P_y равной вероятности реализации уязвимости.

Вероятность реализации угрозы можно рассчитать, исходя из следующей формулы:

$$R(\oplus)Ps = Pt = Pp, \quad (2.2)_y$$

где: P_s – пространственное условие, т.е. вероятность того, что угроза реализуется в том месте, где находится информация;

P_t – временное условие т.е. вероятность того, что угроза реализуется в тот момент, когда информация существует;

P_p – энергетическое условие реализации угрозы, вероятность того, что энергии, для выполнения уязвимости будет достаточно.

Перечисленные условия являются *основными факторами* выполнения уязвимости. Т.е. при невыполнении хотя бы одного из них уязвимость реализовать не возможно. Однако эти условия сами зависят от множества факторов. Факторы, от которых зависит выполнимость основных называются *косвенными*. Состав косвенных факторов, характер их влияния на основные заранее определить не возможно. Поэтому значения вероятностей наступления основных факторов будут вычисляться из значений вероятности наступления косвенных для каждого конкретного случая отдельно.

При вычислении значений основных факторов необходимо помнить, что это вероятностные характеристики и вычисляются по правилам теории вероятности. Таким образом, если основной фактор зависит от одного показателя (косвенного фактора) – *расчет по одному критерию*, то находится он, как отношение величины критерия к его максимальному значению. Проще говоря, меньшее необходимо разделить на большее. О правильности выбора и расчёта вероятности можно судить исходя из простого правила – *значение вероятности всегда должно быть меньше 1*.

Если значение вероятности наступления основного фактора зависит от нескольких критериев, то расчет может производиться либо по *суммовым*, либо по *критическим* критериям. Суммовыми будут критерии, которые вносят определенную долю в вероятность наступления фактора и не зависят друг от друга. При этом необходимо вычислить вероятность наступления каждого из косвенных факторов методом расчета по одному критерию, а затем сложить их, используя следующую формулу:

$$P_{оф} \bigcirc_i \star P_i \bigcirc_i \leftarrow P_i, \quad (2.3)$$

где, $P_{\text{оф}}$ – вероятность наступления основного фактора;

P_i – вероятность наступления косвенного фактора;

i – индекс фактора, n – количество факторов.

Критические – это критерии, которые зависят друг от друга. Т.е. такие критерии, от значения каждого из которых зависит наступление события. Вероятностные показатели этих критериев необходимо перемножить.

$$P_{\text{оф}} \bigcirc \prod_i^n P_i, \quad (2.4)$$

Рассмотри теперь что же является, собственно, самими косвенными факторами и их критериями. *Косвенным фактором* может являться всё, что может привести к реализации угрозы через уязвимость. А критерием является количественный показатель, по которому можно вычислить вероятность наступления этого события.

Например, для бумажного документа, косвенным фактором будет время его хранения. Точнее вероятность утери документа за это время. А критериями этого события могут быть: объем документа (количество листов), температурно-влажностный режим в месте хранения, вероятность кражи и т.д. Для электронной информационной базы данных – объём “винчестера” (или томов), скорость передачи в ЛВС, мощность или быстродействие микропроцессора, объем оперативной памяти и т.д.

Все эти показатели могут быть 3-х типов: технические, статистические и приведённые. *Технические* – это показатели, имеющие свои единицы измерения. Такие показатели, как правило, относятся к характеристикам технических устройств. Они имеют четкое значение в каждый момент времени, область определения или максимальное значение. Определение вероятности наступления неблагоприятного события по этим показателям является наиболее простым. Например, что бы определить вероятность разрушения базы данных на “винчестере”, необходимо объём базы данных разделить на полный объём “винчестера”.

Статистические – это показатели, которые можно определить исходя из статистической информации. Ярким примером служит такой показатель, как время наработки на отказ. Этот показатель определяется в период эксплуатации технического устройства на основании статистики отказов данного устройства.

Приведённые показатели – это показатели, определяемые по качественным оценкам: мало, нормально, много, отлично, хорошо, удовлетворительно, неудовлетворительно и т.п. Оценка их производится методами неформального оценивания. Примером такого показателя может служить лояльность работника своим руководителям.

Рассмотрим, теперь, механизм оценки информационных рисков. На первом этапе необходимо выяснить, какие угрозы характерны для объекта защиты. Их принято делить на 3 больших группы: угрозы доступности, целостности и конфиденциальности информации. Каждая из угроз должна принадлежать к одной из групп. Последовательное рассмотрение каждого множества угроз позволит не “пропустить” какую-нибудь из них.

Далее следует рассмотреть уязвимости, через которые может реализоваться угроза. Любая уязвимость актуальна только тогда, когда выполняются три условия – основные факторы. Последовательное рассмотрение каждого основного фактора позволит составить полный перечень косвенных, и “не пропустить” ни одного из них. Оценка показателей косвенных факторов, в свою очередь, позволит принять адекватное решение по нейтрализации угрозы информационной безопасности.

Сложность механизма оценки угроз обусловлена тем, что он не всегда очевиден и может привести к неэффективным или неадекватным решениям. Приведём пример. При работе в электронной информационной базе данных происходит потеря документов из-за частых сбоев в системе электроснабжения (СЭС). Наиболее очевидным решением является установка устройств бесперебойного питания (УБП). Но помогает это не всегда. Допустим, что к одной линии СЭС подключены и компьютеры, и двигатель системы вентиляции помещения. При включении двигателя в линии происходит падение напряжения. Из-за чего и происходит сбой в работе компьютеров. Использование УБП не помогло, так как из-за частых “скачков” напряжения аккумуляторы УБП быстро разряжаются и УБП выходят из строя. Более эффективным будет замена проводов линии электроснабжения на провода с большим сечением или подключение двигателя и компьютеров к разным линиям.

Рассмотрим эту ситуацию в соответствии с изложенной выше методикой. Угрозой безопасности информации является нестабильное электроснабжение. Уязвимости здесь две:

- 1) недостаточная стабилизация напряжения в СЭС,
- 2) “слабые” характеристики стабилизации напряжения в блоках питания компьютеров.

Для обоих уязвимостей “на лицо” выполнение всех трёх условий - основных факторов:

- 1) пространственный фактор – двигатель и компьютеры подключены к одной линии СЭС;
- 2) временной – двигатель включается и выключается в то же время, когда работают компьютеры;
- 3) энергетический – в момент включения двигателя – энергии для работы компьютеров не хватает.

Выделим множество параметров:

○ по первому фактору: необходимость наличия ПК и двигателя на одной линии питания (приведённый показатель: да/нет);

○ по второму фактору: вероятность одновременной работы двигателя и ПК, рабочее время сотрудников, связанных с работой в базе данных;

○ по третьему фактору: минимальное напряжение стабильной работы ПК, максимально возможная нагрузка в линии СЭС, сечение проводов линии, вероятность сбоя при включении двигателя.

Рассматривая ситуацию в таком порядке, даже без проведения расчетов, становится очевидным нарушение энергетического фактора – подключение двигателя к другой линии СЭС. Нарушение временного фактора едва ли возможно. Для принятия решения по третьему фактору возможно после проведения расчетов.

Практическая часть

Порядок выполнения работы

В ходе работы студенту необходимо решить три задачи:

1. Оценить информационные ресурсы.

2. Выявить косвенные факторы, влияющие на выполнение уязвимостей и составить перечень их параметров.

3. Оценить информационные риски.

Оценка информационных ресурсов производится следующим образом:

1) определяется состав параметров, влияющих на стоимость ресурса.

2) количественные значения приводятся в безразмерный вид. Для этого текущее значение параметра необходимо разделить на его максимальное значение.

3) значения параметров складываются.

Для выполнения второй задачи, студентам необходимо рассмотреть угрозы и уязвимости в информационной системе предприятий, выявленные на предыдущей лабораторной работе. При этом необходимо использовать то предприятие (модель предприятия), которая рассматривалась рабочей группой ранее. Методика выявления факторов и их показателей изложена выше.

Оценка рисков, производится в соответствии с формулами (1) и (2).

Содержание отчета

Отчет по лабораторной работе выполняется на листах белой писчей бумаги формата А4 в печатном виде и должен содержать:

1. Титульный лист;
2. Тему и цель занятия;
3. Оценку информационных ресурсов (таблица 2.1);

Таблица 2.1 - Оценка стоимости ресурса

№ п.п.	Наименование ресурса	Параметры	Значение	Приведённое значение

4. Перечень параметров уязвимостей системы (таблица 2.2);

Таблица 2.2 - Перечень параметров уязвимости системы

№ п.п.	Факторы	Уязвимости	Значение

5. Оценку информационных рисков (таблица 2.3)

Таблица 2.3 - Оценка рисков информационной безопасности

№ п.п.	Уязвимость	Риск

Контрольные вопросы:

1. Что называется угрозой информационной безопасности?
2. Что называется уязвимостью информационной системы?
3. Что называется информационным риском?
4. Дайте понятие основным и косвенным факторам уязвимости информационной системы.
5. Как оценить опасность уязвимости?
6. Какие типы показателей косвенных факторов уязвимости Вы знаете? Для чего они нужны?
7. Что является целью оценки информационных рисков?

Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

Интернет-ресурсы: 1-3

Программное обеспечение: 1-2

Тема 2. Принципы организации и этапы разработки комплексной системы защиты информации

Лабораторная работа 3

Название работы: Разработка моделей объектов защиты

Время 1,5 часа

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Теоретическая часть

Решение проблемы защиты информации с точки зрения системного подхода можно сформулировать как трансформацию существующей системы в требуемую.

Целями системы защиты являются обеспечение требуемых уровней безопасности информации на фирме, в организации, на предприятии (в общем случае – на объекте защиты). Задачи конкретизируют цели применительно к видам и категориям защищаемой информации. А также элементам объекта защиты и отвечают на вопрос, что надо делать для достижения целей. Кроме того, уровень защиты нельзя рассматривать в качестве абсолютной меры, безотносительно от ущерба, который может возникнуть от потери информации и использовании ее злоумышленником во вред владельцу информации.

В качестве ориентира для оценки требуемого уровня защиты информации необходимо определить соотношение между ценой защищаемой информации и затратами на ее защиту. Уровень защиты рационален, когда обеспечивается требуемый уровень безопасности информации ($C_{\text{уи}}$ $C_{\text{уд}}$) и минимизируются расходы на защиту информацию

($C_{\text{зи}}$ $C_{\text{зд}}$). Эти расходы $C_{\text{ри}}$ складываются из:

- затрат на защиту информации $C_{\text{зи}}$;
- ущерба $C_{\text{уи}}$ за счет попадания информации к злоумышленнику и использования ее во вред владельца.

Между этими слагаемыми существует достаточно сложная связь, так как ущерб из-за недостаточной безопасности информации уменьшается с увеличением расходов на ее защиту.

Если первое слагаемое может быть точно определено, то оценка ущерба в условиях скрытности разведки и неопределенности прогноза использования злоумышленником полученной информации представляет достаточно сложную задачу. Ориентировочная оценка ущерба возможна при следующих допущениях.

Владелец информации ожидает получить от ее материализации определенную прибыль, которой он может лишиться в случае попадания ее конкуренту. Кроме того, последний, используя информацию, может нанести владельцу еще дополнительный ущерб за счет, например, изменения тактики, продажи или покупки ценных бума и т.д. Дополнительные

неблагоприятные факторы чрезвычайно трудно поддаются учету. Поэтому в качестве граничной меры для оценки ущерба можно использовать величину потенциальной прибыли $C_{\text{пи}}$, которую ожидает получить от информации ее владелец, т.е.

$$C_{\text{уи}} \geq C_{\text{пи}}, \quad (3.1)$$

В свою очередь величина ущерба зависит от уровня защиты, определяемой расходами на нее. Максимальный ущерб возможен при нулевых расходах на защиту, гипотетически нулевой ущерб обеспечивается при идеальной защите. Но идеальная защита требует бесконечно больших затрат.

При увеличении расходов вероятность попадания информации злоумышленнику, а, следовательно, и ущерб уменьшаются. Но одновременно увеличиваются расходы на защиту. Указанные зависимости иллюстрируются на рисунке 3.1.



Рисунок 3.1 - Зависимость расходов на информацию от затрат на ее защиту

Из рисунка 3.1 следует, что функция $C_{\text{ри}} = f(C_{\text{уи}}, C_{\text{зи}})$ имеет область, в которой $C_{\text{ри}}$ принимает максимальное и минимальное значения. Рост суммарных расходов на информацию с увеличением затрат на ее защиту имеет место в период создания или модернизации системы, когда происходит накопление мер и средств защиты, которые не оказывают существенного влияния на безопасность информации. Например, предотвращение утечки информации по отдельным канал без снижения вероятности утечки по всем остальным не приводит к заметному повышению безопасности информации, хотя затраты на закрытие отдельных каналов могут быть весьма существенными. Образно говоря, для

объекта защиты существует определенная «критическая масса» затрат на защиту информации, при превышении которой эти затраты обеспечивают эффективную отдачу.

При некоторых рациональных затратах на защиту информации выше критических наблюдается минимум суммарных расходов на информацию. При затратах ниже рациональных увеличивается потенциальный ущерб за счет повышения вероятности попадания конфиденциальной информации к злоумышленнику, при более высоких затратах – увеличиваются прямые расходы на защиту.

Ограничения системы представляют собой выделяемые на защиту информации людские, материальные, финансовые ресурсы, а также ограничения в виде требований к системе. Суммарные ресурсы удобно выражать в денежном эквиваленте. Независимо от выделяемых на защиту информации ресурсов они не должны превышать суммарной цены защищаемой информации. Это верхний порог ресурсов.

Проектирование требуемой системы защиты проводится путем системного анализа существующей и разработки вариантов требуемой.

Алгоритм этого процесса включает следующие этапы:

- определение перечня защищаемой информации, целей, задач, ограничений и показателей эффективности системы защиты;
- моделирование существующей системы и выявление ее недостатков с позиции поставленных целей и задач;
- определение и моделирование угроз безопасности информации;
- разработка вариантов (алгоритмов функционирования) проектируемой системы;
- сравнение вариантов по глобальному критерию и частным показателям, выбор наилучших вариантов;
- обоснование выбранных вариантов системы в докладной записке или в проекте для руководства организации;
- доработка вариантов или проекта с учетом замечаний руководства.

Так как отсутствуют формальные способы синтеза системы защиты, то ее оптимизация при проектировании возможна путем постепенного приближения к рациональному варианту в результате нескольких итераций.

В ходе проектирования создаются модели объектов защиты и угроз безопасности информации, в том числе модели каналов утечки информации, оцениваются угрозы, разрабатываются способы защиты информации, выбираются технические средства, определяются эффективность защиты и необходимые затраты. Разработка способов и средств защиты информации прекращается, когда достигается требуемый уровень ее безопасности, а затраты на защиту соответствуют ресурсам.

После рассмотрения руководством предлагаемых вариантов (*лучшие* двух для предоставления выбора), учета предложений и замечаний, наилучший, с точки зрения лица, принимающего решения, вариант (проект, предложения) финансируется и реализуется путем проведения необходимых закупок материалов и оборудования, проведения строительно-монтажных работ, наладки средств защиты и сдачи в эксплуатацию системы защиты.

Следует подчеркнуть, что специалист по защите информации должен при обосновании предлагаемых руководству организации вариантов защиты учитывать психологию лица (руководителя), принимающего решение о реализации предложений, и в большинстве случаев недостаточную информированность его об угрозах безопасности информации в организации.

Психологическим фактором, сдерживающим принятие решения руководителем о выделении достаточно больших ресурсов на защиту информации является то обстоятельство, что в условиях скрытности добывания информации угрозы ее безопасности не представляются достаточно серьезными, а приобретают некоторый абстрактный характер. Знание руководителем о существовании, в принципе, таких угроз, но без достаточно убедительных доводов специалиста о наличии угроз безопасности информации в конкретной организации, не гарантирует финансирование проекта в необходимом объеме. Кроме того, руководитель в силу собственного представления об угрозах, способах и средствах их нейтрализации может преувеличивать значимость одних мер защиты и преуменьшать другие. Однако это обстоятельство не должно уменьшать энтузиазм специалиста по защите информации, так как оно характерно для любого вида деятельности, а умение обосновывать свои предложения является необходимым качеством любого специалиста.

Корректировка мер по защите информации производится после рассмотрения проекта руководством организации, а также в ходе реализации проекта и эксплуатации системы защиты.

Для защиты информации на основе системного подхода и анализа необходимо, наряду с организационным и техническим, методическое обеспечение. В соответствии с алгоритмом проектирования системы оно должно обеспечивать:

- ☐ моделирование объекта защиты;
- ☐ выявление и моделирование угроз безопасности информации;
- ☐ разработку мер инженерно-технической защиты информации.

Моделирование объектов защиты включает: ☐

структурирование защищаемой информации;

- ☐ разработку моделей объектов защиты.

Для структурирования информации в качестве исходных данных используются:

- ☐ перечень сведений, составляющих государственную, ведомственную или коммерческую тайну;
- ☐ перечень источников информации в организации.

Структурирование информации проводится путем классификации информации в соответствии со структурой, функциями и задачами организации с привязкой элементов информации к ее источникам. Детализацию информации целесообразно проводить до уровня, на котором элементу информации соответствует один источник.

Схема классификации разрабатывается в виде графа-структуры, нулевой (верхний) уровень иерархии которой соответствует понятию «защищаемая информация», а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основное требование к схеме классификации - общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня, т. е. одна и та же информация не должна указываться в разных элементах классификации.

Результаты структурирования оформляются в виде:

○ схемы классификации информации; ○ таблицы

3.1.

Таблица разрабатывается на основе схемы классификации информации. В первом столбце указывается номер элемента информации в схеме классификации.

Порядковый номер элемента информации соответствует номеру тематического вопроса в структуре информации. Значность номера равна количеству уровней структуры, а каждая цифра - порядковому номеру тематического вопроса на рассматриваемом уровне среди вопросов, относящихся к одному тематическому вопросу на предыдущем уровне. Например, номер 2635 соответствует информации 5-го тематического вопроса на 4-м уровне, входящего в 3-й укрупненный вопрос 3-го уровня, который, в свою очередь, является частью 6-го тематического вопроса 2-го уровня, представляющего собой вопрос 2-й темы 1-го уровня.

Таблица 3.1 - Результаты структурирования информации

№ элемента информации	Наименование элемента информации	Гриф Конфиденциальности информации	Цена информации	Наименование источника информации	Местонахождение источника информации
1	2	3	4	5	6

Во 2-м, 3-м и 4-м столбцах таблицы указываются наименование элемента информации (тематического вопроса) и его характеристики: гриф и цена. Последующие столбцы таблицы относятся к источникам информации соответствующего ее элемента в схеме классификации. В столбце 5 указывается наименование источника (фамилия человека, название документа или его номер по книге учета, наименование и номер изделия и т.д.), а в графе 6 - места размещения или хранения (возможные рабочие места людей-источников информации, места расположения, размещения или хранения других носителей).

Эти места в общем случае представляют собой:

○ помещения (служебные, лаборатории, офисы, цеха, склады, квартиры и др.);

○ письменные столы рабочих мест сотрудников, хранилища и сейфы, шкафы деревянные и металлические в помещениях.

В помещениях размещается большинство источников информации: люди, документы, разрабатываемая продукция и ее элементы, средства обработки и хранения информации и др., а также источники функциональных и опасных сигналов.

Практическая часть

Вами должно быть выбран и описан конкретный объект защиты. Этим объектом может являться то предприятие, на котором вы работаете или агентство «Недвижимость» (см. информацию для описания в таблице 3.2).

Таблица 3.2 - Наименование и краткое описание объекта защиты

Агентство «Недвижимость», являясь дочерней организацией агентства «Русская недвижимость», расположенного в г. Москве.

В связи с расширением агентство «Недвижимость» предполагает разместиться в помещениях 2-го этажа учреждения, аналогичного помещениям кафедры ОТиЗИ СГУ в аудиториях:

- № 208 (разделенная на две части, в ней - 5 агентов по работе с клиентами, специалист по информационной безопасности);
- № 209 (зал заседаний);
- № 210 (бухгалтер и кассир);
- № 211 (директор и заместитель по работе с кадрами); - холл (секретарша).

Рабочие места каждого сотрудника планируется оборудовать ПЭВМ, объединенными в ЛВС с выходом в Internet.

Вы – специалист по информационной безопасности.

Задание:

1. Необходимо предоставить детальное описание этого предприятия (объем не менее 5 страниц). Описание предприятия должно содержать следующие разделы:

○ общее описание (где находится, чем занимается, сколько человек работает, организационная структура, структура производственных процессов и их краткое описание),

○ нормативная база предприятия, в том числе по защите информации;

○ план территории, расположения помещений/помещения предприятия с указанием наименований соответствующих подразделений, на плане также должны быть указаны основные конструктивные элементы помещений, расположение источников информации, средств ее обработки, линий связи, коммуникации и пр.

○ перечень используемых информационных систем, средств и комплексов защиты.

2. Оформить результаты структурирования информации.

На основании описания предприятия необходимо произвести структурирование информации, обрабатываемой информацией. Результатом выполнения должна быть заполненная таблица 1. Количество элементов информации – не менее 20.

Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

Интернет-ресурсы: 1-3

Программное обеспечение: 1-2

Лабораторная работа 4

Название работы: Структурирование защищаемой информации

Время 1,5 часа

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Теоретическая часть

Структурирование информации проводится путем классификации информации в соответствии со структурой, функциями и задачами организации с привязкой элементов информации к ее источникам. Детализацию информации целесообразно проводить до уровня, на котором элементу информации соответствует один источник.

Результаты структурирования оформляются в виде:

- схемы классификации информации, пример которой приведен на рисунке 4.1;
- таблицы, вариант формы которой приведен в таблице 4.1.

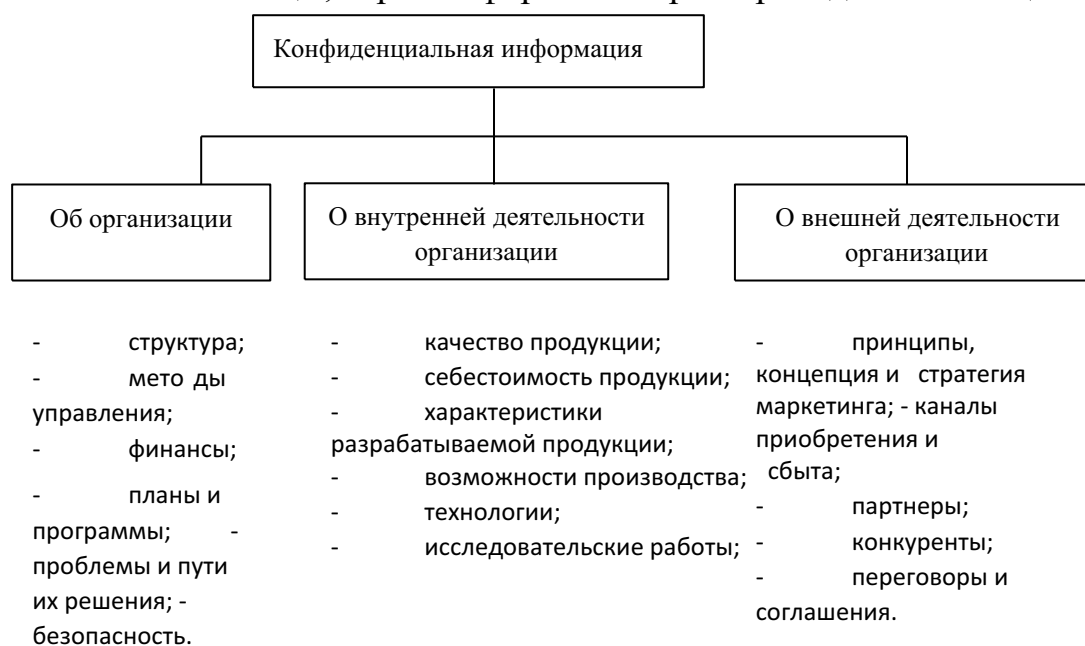


Рисунок 4.1 - Схема классификации информации

Таблица 4.1 - Результаты структурирования

№ элемента информации	Наименование элемента информации	Гриф конфиденциальности информации	Цена Информации	Наименование источника информации	Местонахождение источника информации
1	2	3	4	5	6

Схема классификации разрабатывается в виде графа-структуры, нулевой (верхний) уровень иерархии которой соответствует понятию «защищаемая информация», а n-ый (нижний) - элементам информации одного источника из перечня источников информации организации. Основное требование к схеме классификации - общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня, т. е. одна и та же информация не должна указываться в разных элементах классификации.

Таблица разрабатывается на основе схемы классификации информации. В первом столбце указывается номер элемента информации в схеме классификации. Порядковый номер элемента информации соответствует номеру тематического вопроса в структуре информации. Значимость номера равна количеству уровней структуры, а каждая цифра - порядковому номеру тематического вопроса на рассматриваемом уровне среди вопросов, относящихся к одному тематическому вопросу на предыдущем уровне.

Во 2-м, 3-м и 4-м столбцах таблицы указываются наименование элемента информации (тематического вопроса) и его характеристики: гриф и цена. Последующие столбцы таблицы относятся к источникам информации соответствующего ее элемента в схеме классификации. В столбце 5 указывается наименование источника (фамилия человека, название документа или его номер по книге учета, наименование и номер изделия и т.д.), а в графе 6 - места размещения или хранения (возможные рабочие места людей-источников информации, места расположения, размещения или хранения других носителей).

Эти места в общем случае представляют собой помещения (служебные, лаборатории, офисы, цеха, склады, квартиры и др.); письменные столы

рабочих мест сотрудников, хранилища и сейфы, шкафы деревянные и металлические в помещениях.

В помещениях размещается большинство источников информации: люди, документы, разрабатываемая продукция и ее элементы, средства обработки и хранения информации и др., а также источники функциональных и опасных сигналов.

Для структурирования информации в качестве исходных данных используются:

- ☐ перечень защищаемой информации (приложение А);
- ☐ перечень источников информации в организации.

Тема 3. Факторы влияющие на организацию комплексной системы защиты информации

Лабораторная работа 5

Моделирование технических каналов утечки информации

Время 1,5 часа

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Теоретическая часть

Обнаружение и распознавание каналов утечки информации, так же как любых объектов, производится по их демаскирующим признакам. В качестве достаточно общих признаков или индикаторов каналов утечки информации могут служить указанные в таблице 5.1.

Приведенные индикаторы являются лишь ориентирами при поиске потенциальных каналов утечки. В конкретных условиях их состав существенно больший.

Таблица 5.1 - Признаки или индикаторы каналов утечки информации

Вид канала	Индикаторы
------------	------------

Оптический	Окна, выходящие на улицу, близость к ним противоположных домов и деревьев Отсутствие на окнах занавесок, штор, жалюзей. Просматриваемость содержания документов на столах со стороны окон. дверей, шкафов в помещении Просматриваемость содержания плакатов на стенах помещения для совещания из окон и дверей. Малое расстояние между столами сотрудников в помещении Просматриваемость экранов мониторов ПЭВМ на столах сотрудников со стороны окон, дверей или других сотрудников Складирование продукции во дворе без навесов Малая высота забора и дырки в нем. Переноска и перевозка образцов продукции в открытом виде Появление возле территории организации (предприятия) посторонних людей (в том числе в автомобилях) с биноклями фотоаппаратами, кино и видеокамерами
Вид канала	Индикаторы
Радиоэлектронный	Наличие в помещении радиоэлектронных средств. ПЭВМ ТА городской и внутренней АТС, громкоговорителей трансляционной сети и других предметов Выход окон помещения на улицу, близость к ним улицы и противоположных домов Применение средств радиосвязи Параллельное размещение кабелей в одном жгуте при разводке их внутри здания ч на территории организации. Отсутствие заземления радио и электрических приборов Длительная к частая парковка возле организации чужих автомобилей, в особенности с сидящими в машине людьми

Акустический	Малая толщина дверей и стен помещения Наличие в помещении открытых вентиляционных отверстий Отсутствие экранов на отопительных батареях Близость окон к улице и ее домам. Появление возле организации людей с достаточно большими сумками, длинными и толстыми зонтами Частая и продолжительная парковка возле организации чужих автомобилей
Материально-вещественный	Отсутствие закрытых и опечатанных ящиков для бумаги и твердых отходов с демаскирующими веществами Применение радиоактивных веществ Неконтролируемый выброс газов с демаскирующими веществами, слив в водоемы и вывоз на свалку твердых отходов Запись сотрудниками конфиденциальной информации на неучтенных листах бумаги.

Потенциальные каналы утечки определяются для каждого источника информации, причем их количество может не ограничиваться одним или двумя. Например, от источника информации - руководителя фирмы утечка информации возможна по следующим каналам: - через дверь в приемную или коридор; - через окно на улицу или во двор:

- через вентиляционное отверстие в соседние помещения; - с опасными сигналами по радиоканалу;
- с опасными сигналами по кабелям, выходящим из помещения; - по трубам отопления в другие помещения здания;
- через стены, потолок и пол в соседние помещения; - с помощью закладных устройств за территорию фирмы.

Потенциальные каналы утечки определяются для каждого источника информации, причем их количество может не ограничиваться одним или двумя. Например, от источника информации - руководителя фирмы утечка информации возможна по следующим каналам: - через дверь в приемную или коридор; - через окно на улицу или во двор:

- через вентиляционное отверстие в соседние помещения;
- с опасными сигналами по радиоканалу;
- с опасными сигналами по кабелям, выходящим из помещения; - по трубам отопления в другие помещения здания;
- через стены, потолок и пол в соседние помещения; - с помощью закладных устройств за территорию фирмы.

Все выявленные потенциальные каналы утечки информации и их характеристики записываются в таблицу 5.2.

Наименование источника информации заимствуются из таблицы 5.1. В графе 4 указываются основные элементы среды распространения и возможные места размещения приемника сигналов. По физической природе носителя определяется вид канала утечки информации.

Таблица 5.2 - Потенциальные каналы утечки информации

№ элемента информации	Цена информации	Источник сигнала	Путь утечки информации	Вид канала	Оценки реальности канала	Величина угрозы	Ранг угрозы
1	2	3	4	5	6	7	8

Оценка показателей угроз безопасности представляет достаточно сложную задачу в силу следующих обстоятельств:

- добывание информации нелегальными путями не афишируется и фактически отсутствуют или очень скудно представлены в литературе реальные статистические данные по видам угроз безопасности информации. Кроме того, следует иметь, что характер и частота реализации угроз зависят от криминогенной обстановки в районе нахождения организации и данные об угрозах, например, в странах с развитой рыночной экономикой, не могут быть однозначно использованы для российских условий;
- оценка угроз безопасности информации основывается на прогнозе действий органов разведки. Учитывая скрытность подготовки

и проведения разведывательной операции, их прогноз приходится проводить в условиях острой информационной недостаточности;

- многообразие способов, вариантов и условий доступа к защищаемой информации существенно затрудняют возможность выявления и оценки угроз безопасности информации. Каналы утечки информации могут распространяться на достаточно большие расстояния и включать в качестве элементов среды распространения труднодоступные места;

- априори не известен состав, места размещения и характеристики технических средств добывания информации злоумышленника.

Оценки угроз информации в результате проникновения злоумышленника к источнику или ее утечки по техническому каналу проводятся с учетом меры (вероятности) P_p реализуемости «рассматриваемого пути или канала, а также цены соответствующего элемента информации $C_{ин}$.

Угроза безопасности информации, выраженной в величине ущерба $C_{уи}$ от попадания ее к злоумышленнику, определяется для каждого пути или канала в виде $C_{уи} = C_{ин} * P_p$.

Моделирование угроз безопасности информации завершается их ранжированием в таблицах 5.1 и 5.2.

На каждый потенциальный способ проникновения злоумышленника к источнику информации и канал утечки информации целесообразно завести карточку, в которую заносятся в табличной форме характеристики моделей канала. Структурная, пространственная, функциональная и информационная модели являются приложениями к комплексной модели канала утечки. На этапе разработки способов и средств предотвращения проникновения злоумышленника и утечки информации по рассматриваемому каналу к карточке добавляется приложение с перечнем мер по защите и оценками затрат на нее.

Более удобным вариантом является представление моделей на основе машинных баз данных, математическое обеспечение которых позволяет учесть связи между разными моделями, быстро корректировать данные в них и систематизировать каналы по различным признакам, например, по виду, положению в пространстве, способам и средствам защиты, угрозам.

Практическая часть

Задание:

1. Определить возможные каналы утечки информации для защищаемого объекта.
2. Результаты анализа занести в таблицу 5.2. Указать не менее 10 технических каналов утечки.
3. Графически изобразите на плане предприятия выявленные технические каналы утечки информации.

Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

Интернет-ресурсы: 1-3

Программное обеспечение: 1-2

Лабораторная работа 6

Название работы: Системный анализ информационной безопасности и принятие решения о защите информации правовыми и организационными методами
Время 1,5 часа

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Теоретическая часть

Комплексная система защиты информации создается на объектах для блокирования (парирования) всех возможных или, по крайней мере, наиболее вероятных угроз безопасности информации. Для парирования той или иной угрозы используется определенная совокупность методов и средств защиты. Некоторые из них защищают информацию от нескольких угроз одновременно. Среди методов защиты имеются и универсальные методы, которые являются базовыми при построении любой системы защиты. Это, прежде всего, правовые методы защиты информации, которые служат основой легитимного построения и использования системы защиты

любого назначения. Организационные методы защиты информации, как правило, используются для парирования нескольких угроз. Кроме того, организационные методы используются в любой системе защиты без исключений.

Государство должно обеспечить в стране защиту информации, как в масштабах всего государства, так и на уровне организаций и отдельных граждан. Для решения этой проблемы государство обязано:

- 1) выработать государственную политику безопасности в области информационных технологий;
- 2) законодательно определить правовой статус компьютерных систем, информации, систем защиты информации, владельцев и пользователей информации и т. д.;
- 3) создать иерархическую структуру государственных органов, вырабатывающих и проводящих в жизнь политику безопасности информационных технологий;
- 4) создать систему стандартизации, лицензирования и сертификации в области защиты информации;
- 5) обеспечить приоритетное развитие отечественных защищенных информационных технологий;
- 6) повышать уровень образования граждан в области информационных технологий, воспитывать у них патриотизм и бдительность;
- 7) установить ответственность граждан за нарушения законодательства в области информационных технологий.

В государстве должна проводиться единая политика в области безопасности информационных технологий. В Российской Федерации вопросы информационной безопасности нашли отражение в "Концепции национальной безопасности Российской Федерации", утвержденной Указом Президента РФ № 1300 от 17 декабря 1997 года. В этом документе отмечается, что "в современных условиях всеобщей информатизации и развития информационных технологий резко возрастает значение обеспечения национальной безопасности РФ в информационной сфере". В "Концепции национальной безопасности Российской Федерации" определены важнейшие задачи государства в области информационной безопасности:

* установление необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями ее распространения;

* совершенствование информационной структуры, ускорение развития новых информационных технологий и их широкое внедрение, унификация средств поиска, сбора, хранения и анализа информации с учетом вхождения России в глобальную информационную инфраструктуру; разработка соответствующей нормативной правовой базы и координация, при ведущей роли ФАПСИ, деятельности органов государственной власти и других органов, решающих задачи обеспечения информационной безопасности;

* развитие отечественной индустрии телекоммуникационных и информационных средств, их приоритетное по сравнению зарубежными аналогами распространение на внутреннем рынке;

* защита государственного информационного ресурса и, прежде всего, в федеральных органах государственной власти на предприятиях оборонного комплекса.

Высокие темпы информатизации, а также социальноэкономические изменения в обществе, происшедшие в последние годы, требовали законодательного регулирования отношений, складывающихся в области информационных технологий. Эта проблема во многом была решена принятием Государственной Думой РФ 25 января 1995 года Федерального закона "Об информации, информатизации и защите информации". В законе даны определения основных терминов: информация; информатизация; информационные системы; информационные ресурсы; конфиденциальная информация; собственник и владелец информационных ресурсов; пользователь информации. Государство гарантирует права владельца информации, независимо от форм собственности, распоряжаться ею в пределах, установленных законом. Владелец информации имеет право защищать свои информационные ресурсы, устанавливая режим доступа к ним. В законе определены права и обязанности граждан и государства по доступу к информации. В нем установлен общий порядок разработки и сертификации информационных систем, технологий, средств их обеспечения, а также порядок лицензирования деятельности в сфере информационных технологий. В этом

законе определены цели и режимы защиты информации, а также порядок защиты прав субъектов в сфере информационных процессов и информатизации.

Другим важным правовым документом, регламентирующим вопросы защиты информации в КС, является закон РФ "О государственной тайне". Он принят Постановлением Верховного Совета РФ от 21. 07. 93 г. Закон определяет уровни секретности государственной информации (грифы секретности) и соответствующую степень важности информации. Руководствуясь данным законом и "Перечнем сведений, отнесенных к государственной тайне", введенным в действие Указом Президента РФ от 30 ноября 1995 года, соответствующие государственные служащие устанавливают гриф секретности информации.

На основании приведенных правовых документов ведомства (министерства, объединения, корпорации и т. п.) разрабатывают нормативные документы (приказы, директивы, руководства, инструкции и др.), регламентирующие порядок использования и защиты информации в подведомственных организациях.

Очень важным правовым вопросом является установление юридического статуса КС и особенно статуса информации, получаемой с применением КС. Статус информации или ее правомочность служит основанием для выполнения (невыполнения) определенных действий. Например, в одних АСУ соответствующее должностное лицо имеет юридическое право принимать решения только на основании информации, полученной из АСУ. В других АСУ для принятия решения необходимо получить подтверждающую информацию по другим каналам. В одной и той же АСУ решение может приниматься как с получением подтверждающей информацией, так и без нее. Примером может послужить организация перевода денег с помощью АСУ. До определенной суммы перевод осуществляется автоматически при поступлении соответствующей заявки. Для перевода крупной суммы выполняются дополнительные процедуры проверки правомочности такой операции. Для этого может быть затребована дополнительная информация, в том числе и по дублирующей системе, а окончательное решение о переводе денег может принимать должностное лицо.

Правовой статус информации устанавливается с учетом ее стоимости (важности) и степени достоверности информации, которую способна обеспечить КС.

Важной составляющей правового регулирования в области информационных технологий является установление ответственности граждан за противоправные действия при работе с КС. Преступления, совершенные с использованием КС или причинившие ущерб владельцам компьютерных систем, получили название компьютерных преступлений. В нашей стране 1 января 1997 года введен в действие новый Уголовный кодекс РФ. В него впервые включена глава № 28, в которой определена уголовная ответственность за преступления в сфере компьютерной информации.

В статье 272 предусмотрены наказания за неправомерный доступ к компьютерной информации. За данное деяние предусмотрены наказания, лежащие в диапазоне от денежного штрафа в размере 200 минимальных зарплат до лишения свободы на срок до 5 лет. Отягощающими вину обстоятельствами являются совершение преступления группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети.

Статья 273 устанавливает ответственность за создание, использование и распространение вредоносных (вредительских) программ для ЭВМ. По этой статье предусмотрено наказание от штрафа в размере заработной платы или иного дохода осужденного за два месяца до лишения свободы на срок до семи лет (в зависимости от последствий).

В статье 274 определена ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, если это деяние причинило существенный вред, наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет, либо обязательными работами на срок от ста восьмидесяти до двухсот часов. Если те же деяния повлекли тяжкие последствия, то предусмотрено лишение свободы на срок до 4 лет.

Выработку политики информационной безопасности, подготовку законодательных актов и нормативных документов, организацию

выполнения установленных норм обеспечения безопасности информации осуществляют государственные органы, структура которых приведена на рисунке 6.1.

Возглавляет государственные органы обеспечения информационной безопасности Президент РФ. Он руководит Советом Безопасности и утверждает указы Президента РФ, касающиеся обеспечения безопасности информации в государстве.

Органом исполнительной власти, занимающимся вопросами государственной безопасности, является Совет Безопасности при Президенте РФ. В состав Совета Безопасности входит Межведомственная комиссия по информационной безопасности, которая непосредственно организует обеспечение безопасности в государстве. Комиссия готовит Указы Президента, выступает с законодательной инициативой, координирует деятельность руководителей министерств и ведомств, обеспечивает контроль выполнения политики информационной безопасности в государстве. Рабочим органом Межведомственной комиссии по информационной безопасности является Государственная техническая комиссия при Президенте РФ. Эта комиссия осуществляет подготовку проектов законов, разрабатывает нормативные документы (Решения Государственной технической комиссии), осуществляет сертификацию средств защиты информации (за исключением криптографических средств) и лицензирование деятельности в области производства средств защиты и обучения специалистов по защите информации.



Рисунок 6.1 – Структура государственных органов

Государственная техническая комиссия координирует и направляет деятельность государственных научно-исследовательских учреждений, работающих в области защиты информации. Эта комиссия обеспечивает также работу Межведомственной комиссии по защите государственной тайны, которая координирует деятельность министерств и ведомств по защите государственной тайны. На Межведомственную комиссию по защите государственной тайны возложена задача руководства лицензированием предприятий, учреждений и организаций, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также оказанием услуг по защите государственной тайны. Кроме того, эта комиссия также осуществляет координацию работы по организации сертификации средств защиты информации.

Федеральное агентство правительственной связи и информации при Президенте Российской Федерации (ФАПСИ) обеспечивает правительственную связь и информационные технологии государственного управления. Агентство осуществляет сертификацию всех средств, используемых для организации правительственной связи и информатизации

государственного управления, а также лицензирует все предприятия, учреждения и организации, занимающиеся производством таких средств. Кроме того, в исключительном ведении ФАПСИ находятся вопросы сертификации и лицензирования в области криптографической защиты информации.

В министерствах и ведомствах создаются иерархические структуры обеспечения безопасности информации, которые, как правило, совпадают с организационной структурой министерства (ведомства). Называться они могут по-разному, но функции выполняют сходные.

Усилия государства должны быть направлены на воспитание ответственности граждан за неукоснительное выполнение правовых норм в области информационной безопасности. Необходимо использовать все доступные средства для формирования у граждан патриотизма, чувства гордости за принадлежность к стране, коллективу. Важной задачей государства является также повышение уровня образования граждан в области информационных технологий. Большая роль в этой работе принадлежит образовательной системе государства, государственным органам управления, средствам массовой информации. Это важное направление реализации политики информационной безопасности. Законы и нормативные акты исполняются только в том случае, если они подкрепляются организаторской деятельностью соответствующих структур, создаваемых в государстве, в ведомствах, учреждениях и организациях. При рассмотрении вопросов безопасности информации такая деятельность относится к организационным методам защиты информации.

Организационные методы защиты информации включают меры, мероприятия и действия, которые должны осуществлять должностные лица в процессе создания и эксплуатации КС для обеспечения заданного уровня безопасности информации. Организационные методы защиты информации тесно связаны с правовым регулированием в области безопасности информации. В соответствии с законами и нормативными актами в министерствах, ведомствах на предприятиях, в учреждениях (независимо от форм собственности) для защиты информации в КС создаются специальные службы безопасности (на практике они могут называться и иначе). Эти службы подчиняются, как правило, непосредственно руководству учреждения. Руководители служб

организуют создание и функционирование систем защиты информации. На организационном уровне с использованием средств защиты решаются следующие задачи обеспечения безопасности информации в КС:

- * организация работ по разработке системы защиты информации;
- * ограничение доступа на объект и к ресурсам КС;
- * разграничение доступа к ресурсам КС;
- * планирование мероприятий;
- * разработка документации;
- * воспитание и обучение обслуживающего персонала и пользователей;
- * сертификация и лицензирование;
- * совершенствование системы защиты информации;
- * оценка эффективности функционирования системы защиты информации;
- * контроль выполнения установленных правил работы в КС.

Организационные методы являются стержнем комплексной системы защиты информации в КС. Только с помощью этих методов возможно объединение на правовой основе технических, программных и криптографических средств защиты информации в единую комплексную систему. Конкретные организационные методы защиты информации будут приводиться при рассмотрении парирования угроз безопасности информации. Наибольшее внимание будет уделено организационным мероприятиям при рассматривании вопросов построения и организации функционирования комплексной системы защиты информации.

Практическая часть

Задание:

1. Разработать Примерный перечень исходных данных необходимых для анализа состояния дел по вопросам обеспечения информационной безопасности, разработки предложений по совершенствованию безопасности, разработки предложений по совершенствованию системы защиты и организационно-распорядительных документов.

2. Разработать Соглашение (обязательство) о соблюдении требований обращения с защищаемой информацией.

3. Разработать Инструкцию по организации парольной защиты автоматизированной системы.

Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

Интернет-ресурсы: 1-3

Программное обеспечение: 1-2

Тема 4. Определение и нормативное закрепление состава защищаемой информации **Лабораторная работа 7**

Название работы: Системный анализ информационной безопасности и принятие решения о защите информации от случайных угроз

Время 1,5 часа

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Теоретическая часть

Для блокирования (парирования) случайных угроз безопасности информации в КС должен быть решен комплекс задач.

1. Дублирование информации

Дублирование информации является одним из самых эффективных способов обеспечения целостности информации. Он обеспечивает защиту информации, как от случайных угроз, так и от преднамеренных воздействий.

В зависимости от ценности информации, особенностей построения и режимов функционирования КС могут использоваться различные методы дублирования. Множество методов может быть классифицировано по различным признакам.

По времени восстановления информации методы дублирования могут быть разделены на:

- оперативные; - неоперативные.

К оперативным методам относятся методы дублирования информации, которые позволяют использовать дублирующую информацию в реальном масштабе времени. Это означает, что переход к использованию дублирующей информации осуществляется за время, которое позволяет выполнить запрос на использование информации в режиме реального времени для данной КС. Все методы, не обеспечивающие выполнения этого условия, относят к неоперативным методам дублирования.

По используемым для целей дублирования средствам методы дублирования можно разделить на методы, использующие:

- дополнительные внешние запоминающие устройства (блоки);
- специально выделенные области памяти на несъемных машинных носителях;

- съемные носители информации.

По числу копий методы дублирования делятся на: -
одноуровневые;

- многоуровневые.

Как правило, число уровней не превышает 3.

По степени пространственной удаленности носителей основной и дублирующей информации методы дублирования могут быть разделены на методы:

- сосредоточенного дублирования; - рассредоточенного дублирования.

Для определённости целесообразно считать методами сосредоточенного дублирования такие методы, для которых носители с основной и дублирующей информацией находятся в одном помещении. Все другие методы относятся к рассредоточенным.

В соответствии с процедурой дублирования различают методы:
полного копирования; - зеркального копирования; - частичного копирования;

- комбинированного копирования.

При полном копировании дублируются все файлы.

При зеркальном копировании любые изменения основной информации сопровождаются такими же изменениями и дублирующей информации. При таком дублировании основная информация и дубль всегда идентичны.

Частичное копирование предполагает создание дублей определенных файлов, например, файлов пользователя. Одним из видов частичного копирования, получившим название инкрементного копирования, является метод создания дублей файлов, измененных со времени последнего копирования.

Комбинированное копирование допускает комбинации, например, полного и частичного копирования с различной периодичностью их проведения.

Наконец, по виду дублирующей информации методы дублирования разделяются на:

- методы со сжатием информации; -
методы без сжатия информации.

В качестве внешних запоминающих устройств для хранения дублирующей информации используются накопители на жестких магнитных дисках и магнитных лентах. Накопители на жестких магнитных дисках применяются обычно для оперативного дублирования информации. Идеология надежного и эффективного хранения информации на жестких дисках нашла свое отражение в так называемой технологии RAID (Redundant Array of Independent Disks). Эта технология реализует концепцию создания блочного устройства хранения данных с возможностями параллельного выполнения запросов и восстановления информации при отказах отдельных блоков накопителей на жестких магнитных дисках. Устройства, реализующие эту технологию, называют подсистемами RAID или дисковыми массивами RAID.

Технология RAID явилась результатом развития технологий надежного хранения информации на жестких дисках, которые применяются и сейчас. Наиболее простым методом дублирования данных в КС является использование выделенных областей памяти на рабочем диске. Таким образом, дублируется наиболее важная системная информация. Например, таблицы каталогов и таблицы файлов дублируются таким образом, чтобы они были размещены на цилиндрах и поверхностях жесткого диска (пакета дисков), отличных от тех, на которых находятся рабочие таблицы. Такое дублирование защищает от полной потери информации при повреждении отдельных участков поверхности дисков.

Очень надежным методом оперативного дублирования является использование зеркальных дисков. Зеркальным называют жесткий магнитный диск отдельного накопителя, на котором хранится информация полностью идентичная информации на рабочем диске. Достигается это за счет параллельного выполнения всех операций записи на оба диска. При отказе рабочего накопителя автоматически осуществляется переход на работу с зеркальным диском практически без потерь времени при полной сохранности информации.

Для особо ответственных применений (военные системы, АСУ технологическими процессами, серверы сетей и некоторые другие) могут использоваться более одного резервного диска, подключенных к отдельным контроллерам и блокам питания. Зеркальное дублирование обеспечивает

надежное оперативное дублирование, но требует, как минимум, вдвое больших аппаратных затрат.

Зеркальное дублирование предусматривается на 1-м уровне RAID. Всего в технологии RAID выделяется 6 основных уровней с 0-го по 5-й. С учетом различных модификаций их может быть больше. Уровни RAID определяют порядок записи на независимые диски и порядок восстановления информации. Различные уровни RAID обеспечивают различное быстродействие подсистемы и различную эффективность восстановления информации. 0-ой уровень RAID предполагает поочередное использование блоков (накопителей на магнитных дисках) для записи файлов. Дублирование не используется. На 2-ом уровне биты информации поочередно размещаются на дисках. Данные размещаются на дисках с дублированием. Начиная с 3-го уровня, для восстановления информации используется не дублирование данных, а контрольная информация. Восстановление возможно при отказе одного диска. На 3-м уровне байты данных поочередно записываются на диски. Контрольная информация (контрольные суммы) записывается на один выделенный диск. Начиная с 4-го уровня, поочередная запись на диски ведется блоками. На 4-м уровне для записи контрольной информации отводится выделенный диск. Подсистема 4-го уровня допускает параллельное выполнение запросов на чтение, но запись осуществляется последовательно, так как контрольная информация записывается на один диск. На 5-м уровне осуществляется поочередная запись на диски, как блоков данных, так и контрольной информации. На этом уровне возможно осуществлять одновременно несколько операций чтения или записи. В случае отказа одного диска он восстанавливается с помощью контрольной информации. Для восстановления информации с отказавшего диска требуется до 10 минут времени.

Блочная конструкция подсистем RAID позволяет наращивать число дисков. Реальные подсистемы поддерживают несколько уровней, которые выбираются пользователем с учетом требований, предъявляемых к ВЗУ конкретной КС. В подсистемах RAID, как правило, используются резервные источники питания, что существенно повышает отказоустойчивость таких подсистем.

Для дублирования информации используются также накопители на магнитных лентах. Такие устройства обладают большой емкостью, но значительно уступают накопителям на магнитных дисках по времени доступа к информации.

В настоящее время для хранения дублирующей информации используются устройства, получившие название ленточные системы с автоматической сменой кассет. Их называют также библиотеками. Такие системы состоят из одного или нескольких лентопротяжных механизмов, механизма перемещения кассет и магазина для кассет. На одной кассете может храниться 10 Гбайт сжатой или 4 Гбайта несжатой информации. Если учесть, что в магазине системы может находиться до 60 кассет (Spectra Logic 4655), то емкость таких систем позволяет хранить огромные массивы данных. Наряду с такими мощными системами могут использоваться и компактные системы с емкостью магазина в несколько кассет. Например, ленточная система Conner Peripherals 4586 NP имеет магазин емкостью 4 кассеты. С учетом возможности замены кассет такие системы позволяют дублировать на ленты объемы информации, ограниченные только наличием свободных кассет. Как правило, библиотеки используются для неоперативного дублирования. Поэтому информация на ленты обычно записывается в сжатом виде. С помощью этих устройств осуществляется полное, частичное и комбинированное копирование с созданием копий различных уровней.

Съемные машинные носители могут использоваться для дублирования информации без использования специальных аппаратных средств. Для этих целей используются, как правило, гибкие магнитные диски, оптоэлектронные диски, а также жесткие съемные магнитные диски и магнитные ленты.

Методы использования съемных носителей информации сходны с методами использования ленточных систем с автоматической сменой кассет.

При использовании многоуровневого дублирования может быть реализован следующий подход к созданию и использованию копий. В качестве эталона верхнего уровня используется редко изменяемая информация (программы, постоянные исходные данные). Носитель с этой информацией используется только для восстановления информации, если ее

невозможно восстановить с РГ эталонов более низкого уровня, а также при изменениях информации и при периодическом контроле. Эталон второго уровня получается путем полного копирования информации с определенной периодичностью, например, один раз в сутки. На эталон первого уровня осуществляется инкрементное копирование либо по времени (раз в смену), либо после существенных и важных изменений. Например, получение важных сообщений по сети или результатов выполнения программ.

Распределенное копирование достижимо в компьютерных сетях и является практически единственным способом обеспечения целостности и доступности информации при стихийных бедствиях и крупных авариях.

2. Повышение надежности компьютерных сетей

Под надежностью понимается свойство системы выполнять возложенные на нее задачи в определенных условиях эксплуатации. При наступлении отказа компьютерная система не может выполнять все предусмотренные документацией задачи, т.е. переходит из исправного состояния в неисправное. Если при наступлении отказа КС способна выполнять заданные функции, сохраняя значения основных характеристик в пределах, установленных технической документацией, то система находится в работоспособном состоянии.

С точки зрения обеспечения безопасности информации необходимо сохранять хотя бы работоспособное состояние КС. Для решения этой задачи необходимо обеспечить высокую надежность функционирования алгоритмов, программ и технических (аппаратных) средств. Поскольку алгоритмы в КС реализуются за счет выполнения программ или аппаратным способом, то надежность алгоритмов отдельно не рассматривается. В этом случае считается, что надежность КС обеспечивается надежностью программных и аппаратных средств.

Надежность КС достигается за счет решения комплекса задач на этапах:

- разработки;
- производства; эксплуатации.

Для программных средств рассматриваются этапы разработки и эксплуатации. Этап разработки является определяющим при создании надежных систем.

На этом этапе основными направлениями повышения надежности программных средств являются:

- корректная постановка задачи на разработку;
- использование прогрессивных технологий программирования;
- контроль правильности функционирования.

Корректность постановки задачи достигается в результате совместной работы специалистов предметной области и высокопрофессиональных программистов-алгоритмистов.

В настоящее время для повышения качества программных продуктов используются современные технологии программирования (например, CASE технология). Эти технологии позволяют значительно сократить возможности внесения субъективных ошибок разработчиков. Они характеризуются высокой автоматизацией процесса программирования, использованием стандартных программных модулей, широкими возможностями комплексирования этих модулей и тестирования их совместной работы.

Контроль правильности функционирования алгоритмов и программ осуществляется на каждом этапе разработки и завершается комплексным контролем, охватывающим все решаемые задачи и режимы.

На этапе эксплуатации программные средства дорабатываются, в них устраняются замеченные ошибки. Поддерживается целостность программных средств и актуальность данных, используемых этими средствами.

Надежность технических средств (ТС) КС обеспечивается на всех этапах. На этапе разработки выбираются элементная база, технология производства и структурные решения, обеспечивающие максимально достижимую надежность КС в целом.

Велика роль в процессе обеспечения надежности ТС и этапа производства. Главными условиями выпуска надежной продукции являются высокий технологический уровень производства и организация эффективного контроля качества выпускаемых ТС.

Удельный вес этапа эксплуатации ТС в решении проблемы обеспечения надежности КС в последние годы значительно снизился. Для определённых видов вычислительной техники, таких как персональные ЭВМ, уровень требований к процессу технической эксплуатации снизился практически до уровня эксплуатации бытовых приборов. Второй особенностью нынешнего этапа эксплуатации средств вычислительной

техники является сближение эксплуатации технических и программных средств (особенно средств общего программного обеспечения). Тем не менее, роль этапа эксплуатации ТС остается достаточно значимой в решении задачи обеспечения надежности КС и, прежде всего, надежности сложных систем.

3. Создание отказоустойчивых компьютерных сетей

Отказоустойчивость - это свойство КС сохранять работоспособность при отказах отдельных устройств, блоков, схем. Известны три основных подхода к созданию отказоустойчивых систем:

- простое резервирование;
- помехоустойчивое кодирование информации;
- создание адаптируемых систем.

Любая отказоустойчивая система обладает избыточностью. Одним из наиболее простых и действенных путей создания отказоустойчивых систем является простое резервирование. Простое резервирование основано на использовании устройств, блоков, узлов, схем только в качестве резервных. При отказе основного элемента осуществляется переход на использование резервного. Резервирование осуществляется на различных уровнях: на уровне устройств, на уровне блоков, узлов и т. д. Резервирование отличается также и глубиной. Для целей резервирования могут использоваться один резервный элемент и более. Уровни и глубина резервирования определяют возможности системы парировать отказы, а также аппаратные затраты. Такие системы должны иметь несложные аппаратно-программные средства контроля работоспособности элементов и средства перехода на использование, при необходимости, резервных элементов. Примером резервирования может служить использование "зеркальных" накопителей на жестких магнитных дисках. Недостатком простого резервирования являются значительные затраты средств, которые используются только для повышения отказоустойчивости.

Помехоустойчивое кодирование основано на использовании информационной избыточности. Рабочая информация в КС дополняется определенным объемом специальной контрольной информации. Наличие этой контрольной информации (контрольных двоичных разрядов) позволяет путем выполнения определенных действий над рабочей и контрольной информацией определять ошибки и даже исправлять их. Так как ошибки

являются следствием отказов средств КС, то, используя исправляющие коды, можно парировать часть отказов. Исправляющие возможности кодов для конкретного метода помехоустойчивого кодирования зависят от степени избыточности. Чем больше используется контрольной информации, тем шире возможности кода по обнаружению и исправлению ошибок. Ошибки характеризуются кратностью, т.е. количеством двоичных разрядов, в которых одновременно искажено содержимое. Помехоустойчивые коды обладают различными возможностями по обнаружению и исправлению ошибок различной кратности. Так классический код Хемминга обнаруживает и исправляет однократные ошибки, а двукратные ошибки - только обнаруживает.

Помехоустойчивое кодирование наиболее эффективно при парировании самоустраниющихся отказов, называемых сбоями. Помехоустойчивое кодирование при создании отказоустойчивых систем, как правило, используется в комплексе с другими подходами повышения отказоустойчивости.

Наиболее совершенными системами, устойчивыми к отказам, являются адаптивные системы. В них достигается разумный компромисс между уровнем избыточности, вводимым для обеспечения устойчивости (толерантности) системы к отказам, и эффективностью использования таких систем по назначению.

В адаптивных системах реализуется так называемый принцип элегантной деградации. Этот принцип предполагает сохранение работоспособного состояния системы при некотором снижении эффективности функционирования в случаях отказов ее элементов.

Адаптивные системы содержат аппаратно-программные средства для автоматического контроля работоспособности элементов системы и осуществления ее реконфигурации при возникновении отказов элементов. При реконфигурации восстанавливается необходимая информация (при ее утрате), отключается отказавший элемент, осуществляется изменение связей и режимов работы элементов системы. Простым примером адаптивной КС может служить ЭВМ, имеющая в своем составе математический и графический сопроцессоры, а также оперативную память блочной структуры. Все сопроцессоры и блоки памяти используются для достижения максимальной производительности ЭВМ. При отказе

какоголибо сопроцессора он логически отключается от ЭВМ, а его функции выполняет центральный процессор. При этом система деградирует, так как снижается производительность ЭВМ. Но в то же время система сохраняет работоспособность и может завершить вычислительный процесс. При отказе блока оперативной памяти он отключается, и емкость памяти уменьшается. Чтобы избежать потерь информации при отказах процессоров и блоков ' оперативной памяти, вычислительный процесс возобновляется либо сначала, либо с последней контрольной точки. Механизм контрольных точек используется обычно при выполнении сложных трудоемких программ. Он заключается в запоминании всей необходимой информации для возобновления выполнения программы с определенной точки. Запоминание осуществляется через определенные интервалы времени.

В адаптивных системах даже внешние устройства не используются только как резервные. Информация, необходимая для восстановления данных с отказавшего ВЗУ, хранится на накопителях, которые используются для хранения и рабочей информации. Примером таких систем являются RAID системы.

4. Блокировка ошибочных операций

Ошибочные операции или действия могут вызываться отказами аппаратных и программных средств, а также ошибками пользователей и обслуживающего персонала. Некоторые ошибочные действия могут привести к нарушениям целостности, доступности и конфиденциальности информации. Ошибочная запись в ОП и на ВЗУ, нарушение разграничения памяти при мультипрограммных режимах работы ЭВМ, ошибочная выдача информации в канал связи, короткие замыкания и обрыв проводников - вот далеко не полный перечень ошибочных действий, которые представляют реальную угрозу безопасности информации в КС.

Для блокировки ошибочных действий используются технические и аппаратно-программные средства.

Технические средства используются в основном для предотвращения ошибочных действий людей. К таким средствам относятся блокировочные тумблеры, защитные экраны и ограждения, предохранители, средства блокировки записи на магнитные ленты и магнитные дискеты.

Аппаратно-программные средства позволяют, например, блокировать вычислительный процесс при нарушениях программами адресных

пространств оперативной памяти с помощью граничных регистров или ключей защиты. При мультипрограммных режимах работы ЭВМ оперативная память распределяется между программами. Приведенный механизм позволяет сравнивать адреса команд активной программы с границами разрешенной области ОП для этой программы и блокировать обращение при нарушении границ. Аппаратно-программные средства используются также для блокирования выдачи информации в неразрешенные каналы связи, запрета выполнения операций, которые доступны только в определенных режимах, например, в режиме работы операционной системы. С помощью аппаратно-программных средств может быть заблокирована запись в определенные области внешних запоминающих устройств и некоторые другие операции.

На программном уровне могут устанавливаться атрибуты файлов, в том числе и атрибут, запрещающий запись в файлы. С помощью программных средств устанавливается режим обязательного подтверждения выполнения опасных операций, таких как уничтожение файлов, разметка или форматирование ВЗУ и другие.

5. Оптимизация взаимодействия человека с компьютерной сетью

Одним из основных направлений защиты информации в КС от непреднамеренных угроз является сокращения числа ошибок пользователей и обслуживающего персонала, а также минимизация последствий этих ошибок. Для достижения этих целей необходимы:

- научная организация труда человека;
- воспитание и обучение пользователей и персонала;
- анализ и совершенствование процессов взаимодействия человека с КС.

Научная организация труда предполагает:

- оборудование рабочих мест;
- оптимальный режим труда и отдыха;
- дружественный интерфейс (связь, диалог) человека с КС.

Рабочее место пользователя или специалиста из числа обслуживающего персонала должно быть оборудовано в соответствии с рекомендациями эргономики. Освещение рабочего места; температурновлажностный режим; расположение табло, индикаторов,

клавиш и тумблеров управления; размеры и цвет элементов оборудования, помещения; положение пользователя (специалиста) относительно оборудования; использование защитных средств -все это должно обеспечивать максимальную производительность человека в течение рабочего дня. Одновременно сводится к минимуму утомляемость работника и отрицательное воздействие на его здоровье неблагоприятных факторов производственного процесса. Для людей, работающих с КС, основными неблагоприятными факторами являются: излучения мониторов, шумы электромеханических устройств, гиподинамия, и, как правило, высокие нагрузки на нервную систему. Вредные воздействия устройств постоянно уменьшаются за счет совершенствования самих устройств и в результате использования защитных экранов. Последствия гиподинамии (малоподвижного, статического положения человека на рабочем месте) и высокие нагрузки на нервную систему компенсируются оптимальным режимом труда и отдыха, а также совершенствованием процесса общения человека с КС. Так при работе с ЭВМ медики рекомендуют 10-15 минутные перерывы через каждый час работы. Во время перерывов следует выполнять физические упражнения и упражнения на снятие психических нагрузок. Продолжительность работы с использованием монитора не должна превышать 6 часов за рабочий день. При сменной организации труда после 6 часов работы должен предоставляться отдых, продолжительность которого определяется длительностью смены.

Прогресс в области электронной вычислительной техники позволил значительно облегчить взаимодействие человека с ЭВМ.

Если на заре внедрения ЭВТ с компьютером мог работать только человек с высшим специальным образованием, то теперь на ПЭВМ работают дети дошкольного возраста. Дальнейшее развитие интерфейса человека с КС идет в направлении совершенствования процессов ввода-вывода информации и управления вычислительным процессом. Речевой ввод информации, автоматический ввод-вывод видео- и аудиоинформации, работа с графикой, вывод информации на экраны и табло создают новые возможности для общения человека с КС. Очень важным для обеспечения безопасности информации является совершенствование диалога пользователя с КС. Наличие развитых систем меню, блокировок неправильных действий, механизма напоминаний, справочных систем,

систем шаблонов существенно снимает нагрузку на нервную систему, сокращает число ошибок, повышает работоспособность человека и производительность системы в целом.

Одним из центральных вопросов обеспечения безопасности информации в КС от всех классов угроз (в том числе и от преднамеренных) является вопрос воспитания и обучения, прежде всего, обслуживающего персонала, а также пользователей корпоративных КС. В КС общего назначения работа с пользователями затруднена и сводится, главным образом, к контролю за их деятельностью.

У обслуживающего персонала и пользователей КС необходимо воспитывать такие качества как патриотизм (на уровне государства и на уровне корпорации), ответственность, аккуратность и др. Чувство патриотизма воспитывается у граждан страны за счет целенаправленной политики государства и реального положения дел в стране. Успешная политика государства внутри страны и на международной арене способствует воспитанию у граждан патриотизма, гордости за свое отечество. Не меньшее значение, особенно для негосударственных учреждений, имеет воспитание корпоративного патриотизма. В коллективе, где ценится трудолюбие, уважительное отношение друг к другу, поощряется аккуратность, инициатива и творчество, у работника практически не бывает внутренних мотивов нанесения вреда своему учреждению. Важной задачей руководства является также подбор и расстановка кадров с учетом их деловых и человеческих качеств. Большой положительный опыт воспитания корпоративного патриотизма накоплен в Японии, где очень удачно соединяются мировой опыт управления коллективами и национальные особенности японского народа.

Наряду с воспитанием специалистов большое значение в деле обеспечения безопасности информации в КС имеет и обучение работников. Дальновидный руководитель не должен жалеть средств на обучение персонала. Обучение может быть организовано на различных уровнях. Прежде всего, руководство должно всемерно поощрять стремление работников к самостоятельному обучению. Важно обучать наиболее способных, трудолюбивых работников в учебных заведениях, возможно и за счет учреждения.

Важной задачей оптимизации взаимодействия человека с КС является также анализ этого процесса и его совершенствование. Анализ должен проводиться на всех жизненных этапах КС и направляться на выявление слабых звеньев. Слабые звенья заменяются или совершенствуются как в процессе разработки новых КС, так и в процессе модернизации существующих.

6. Минимизация ущерба от аварий и стихийных бедствий

Стихийные бедствия и аварии могут причинить огромный ущерб объектам КС. Предотвратить стихийные бедствия человек пока не в силах, но уменьшить последствия таких явлений во многих случаях удастся. Минимизация последствий аварий и стихийных бедствий для объектов КС может быть достигнута путем:

- правильного выбора места расположения объекта;
- учета возможных аварий и стихийных бедствий при разработке и эксплуатации КС;
- организации своевременного оповещения о возможных стихийных бедствиях;
- обучение персонала борьбе со стихийными бедствиями, авариями и ликвидации их последствий.

Объекты КС по возможности должны располагаться в тех районах, где не наблюдается таких стихийных бедствий как наводнения, землетрясения. Объекты необходимо размещать вдалеке от таких опасных объектов как нефтебазы и нефтеперерабатывающие заводы, склады горючих и взрывчатых веществ, плотин и т. д.

На практике далеко не всегда удастся расположить объект вдалеке от опасных предприятий или районов с возможными стихийными бедствиями. Поэтому при разработке, создании и эксплуатации объектов КС необходимо предусмотреть специальные меры. В районах с возможными землетрясениями здания должны быть сейсмостойкими. В районах возможных затоплений основное оборудование целесообразно размещать на верхних этажах зданий. Все объекты должны снабжаться автоматическими системами тушения пожара. На объектах, для которых вероятность стихийных бедствий высока, необходимо осуществлять распределенное дублирование информации и предусмотреть возможность перераспределения функций объектов. На всех объектах должны

предусматриваться меры на случай аварии в системах электропитания. Для объектов, работающих с ценной информацией, требуется иметь аварийные источники бесперебойного питания и подвод электроэнергии производить не менее чем от двух независимых линий электропередач. Использование источников бесперебойного питания обеспечивает, по крайней мере, завершение вычислительного процесса и сохранение данных на внешних запоминающих устройствах. Для малых КС такие источники способны обеспечить работу в течение нескольких часов.

Потери информационных ресурсов могут быть существенно уменьшены, если обслуживающий персонал будет своевременно предупрежден о надвигающихся природных катаклизмах. В реальных условиях такая информация часто не успевает дойти до исполнителей. Поэтому персонал должен быть обучен действиям в условиях стихийных бедствий и аварий, а также уметь восстанавливать утраченную информацию.

Практическая часть

Задание:

1. Изучить комплекс задач, который должен быть решен для блокирования (парирования) случайных угроз безопасности информации в КС.
2. Составить классификацию методов блокирования (парирования) случайных угроз безопасности информации в КС зависимости от ценности информации, особенностей построения и режимов функционирования КС.
3. Для объекта защиты из игровой ситуации предложите комплекс мероприятий (не менее 10) для парирования случайных угроз безопасности информации.

Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

Интернет-ресурсы: 1-3

Программное обеспечение: 1-2

Лабораторная работа 8

Название работы: Системный анализ информационной безопасности и принятие решения по защите информации от традиционного шпионажа и диверсий
Время 1,5 часа

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Теоретическая часть

При защите информации в КС от традиционного шпионажа и диверсий используются те же средства и методы защиты, что и для защиты других объектов, на которых не используются КС. Для защиты объектов КС от угроз данного класса должны быть решены следующие задачи:

- создание системы охраны;
- ограничения работ с конфиденциальными информационными ресурсами на объекте КС;
- противодействие наблюдению;
- противодействие подслушиванию;
- защита от злоумышленных действий персонала.

Объект, на котором производятся работы с ценной конфиденциальной информацией, имеет, как правило, несколько рубежей защиты:

- контролируемая территория;
- здание;
- помещение;
- устройство, носитель информации;
- программа;
- информационные ресурсы.

Состав системы охраны зависит от охраняемого объекта. В общем случае система охраны объекта (СОО) КС должна включать следующие компоненты:

- инженерные конструкции;
- охранная сигнализация;
- средства наблюдения; - подсистема доступа на объект; - дежурная смена охраны.

Инженерные конструкции служат для создания механических препятствий на пути злоумышленников. Они создаются оп периметру контролируемой зоны.

В здания и помещения злоумышленники пытаются проникнуть, как правило, через двери или окна. Поэтому с помощью инженерных конструкций укрепляется, прежде всего, это слабое звено в защите объекта.

Охранная сигнализация служит для обнаружения попыток несанкционированного проникновения на охраняемый объект. Системы охранной сигнализации должны отвечать следующим требованиям:

- охват контролируемой зоны по всему периметру;
- высокая чувствительность к действиям злоумышленников;
- надежная работа в любых погодных и временных условиях;
- устойчивость к естественным помехам;
- быстрота и точность определения места нарушения; - возможность централизованного контроля событий.

Организация непрерывного наблюдения или видеоконтроля за объектом является одной из основных составляющих системы охраны объекта. В современных условиях функция наблюдения за объектом реализуется с помощью систем замкнутого телевидения (телевизионных систем видеоконтроля).

Доступ на объект осуществляется на контрольно-пропускных пунктах (КПП), проходных, через контролируемый вход в здания и помещения. На КПП и проходных дежурят контролеры из состава дежурной смены охраны. Входы в здания и помещения может контролироваться только техническими средствами. Проходные, КПП, входы в здания и помещения оборудуются средствами автоматизации и контроля доступа. Одной из основных задач, решаемых при организации допуска на объект, является идентификация и аутентификация лиц, допускаемых на объект.

Состав дежурной смены, его экипировка, место размещения определяется статусом охраняемого объекта. Используемая охранную сигнализацию, системы наблюдения и автоматизации доступа, дежурная смена охраны обеспечивает только санкционированный доступ на объект и в охраняемые помещения. Дежурная смена может находиться на объекте

постоянно или прибывать на объект при получении сигналов тревоги от системы сигнализации и наблюдения.

Практическая часть

Задание:

1. Разработать систему охраны объекта КС для предотвращения несанкционированного проникновения на территорию и в помещения объекта посторонних лиц, обслуживающего персонала и пользователей.

2. Предложить меры:

- по организации работы с конфиденциальными ресурсами на объектах

КС;

- по противодействию наблюдению в оптическом диапазоне;
- по противодействию подслушиванию;
- по борьбе с закладными подслушивающими устройствами;
- по защите от злоумышленных действий обслуживающего персонала и пользователей.

Пример ответа

Система охраны объекта

1. Инженерные конструкции

Охраняемый объект оборудован отечественной автоматизированной системой контроля доступа в помещения «Полонез», на базе электронных замков. Все замки от входных дверей объединены в единую автоматизированную систему, информация от которой поступает на ПЭВМ к начальнику службы безопасности.

На окна установлены решетки с диаметром прутьев не менее 10 мм, расстояние между ними не менее 120 мм, а глубина заделки прутьев в стену – не менее 200 мм.

2. Охранная сигнализация

На окна установлены удароконтактные датчики типа УДК-1М; помещения оборудованы активными акустическими (ультразвуковыми) датчиками (ДУЗ-12, «Эхо-3»), позволяющими не только обнаруживать злоумышленников, но и возгорания в закрытых помещениях.

Вход в комплекс оборудован телевизионным датчиком (телевизионной камерой типа VM 216 фирмы Retan) для контроля в нерабочее время.

Вся информация поступает на пульт дежурной смены охраны по СГУ.

3. Средства наблюдения

Телевизионная камера для контроля за входной дверью внутри комплекса с монитора начальника службы безопасности в рабочее время.

4. Средства доступа на объект

Пластиковые штриховые карты для электронных замков.

5. Дежурная смена охраны

Дежурная смена СГУ прибывает на объект при получении сигналов тревоги от системы сигнализации и наблюдения.

Меры по организации работы с конфиденциальными ресурсами на объектах КС:

- определение и оборудование места хранения конфиденциальных информационных ресурсов и места работы с ними;
- установление порядка учета, выдачи, работы им сдачи на хранение конфиденциальных ресурсов;
- назначение исполнителей с определением их обязанностей;
- организация сбора и уничтожения ненужных документов и списанных машинных носителей;
- организация контроля за выполнением установленного порядка работы с конфиденциальными ресурсами.

Меры по противодействию наблюдению в оптическом диапазоне:

- использование оконных стекол с односторонней проводимостью;
- применение штор и защитного окрашивания стекол;
- размещение рабочих столов, мониторов, табло и плакатов таким образом, чтобы они не просматривались через окна или открытые двери;
- необходимо, чтобы двери были закрыты;
- расположение столов и мониторов ЭВМ должно исключать возможность наблюдения документов или выдаваемой информации на соседнем столе или мониторе;
- стенды с конфиденциальной информацией должны иметь шторы.

Меры по противодействию подслушиванию:

1) методы защиты речевой информации при передаче ее по каналам связи:

- аналоговое скремблирование:

- а) частотная инверсия спектра (маскиратор);

- б) частотная инверсия спектра сигнала со смещением несущей частоты;

- в) разбиение полосы частот речевого сигнала на поддиапазоны с последующей перестановкой и инверсией;

- г) временное скремблирование; - дискретизация речевой информации;

2) методы защиты от прослушивания акустических сигналов в помещениях:

- звукоизоляция и звукопоглощение акустического сигнала;

- зашумление помещений или твердой среды для маскировки акустических сигналов;

- защиты от несанкционированной записи речевой информации на диктофон;

- обнаружение и изъятие закладных устройств.

Меры по борьбе с закладными подслушивающими устройствами:

- средства радиоконтроля помещений: а) обнаружители поля;

- б) бытовые радиоприемники;

- в) специальные радиоприемники;

- г) автоматизированные комплексы;

- средства поиска неизлучающих закладок:

- устройства нелинейной локации;

- обнаружители пустот;

- металлодетекторы;

- рентгеновские установки;

- средства подавления закладных устройств:

- генераторы помех;

- средства нарушения функционирования закладок; - средства разрушения закладок.

Меры по защите от злоумышленных действий обслуживающего персонала и пользователей:

- получение всеми доступными законными путями информации о своих сотрудниках, о людях или организациях, представляющих потенциальную угрозу информационным ресурсам;
- контроль выполнения установленных мер безопасности;
- создание и поддержание в коллективе здорового нравственного климата.

Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

Интернет-ресурсы: 1-3

Программное обеспечение: 1-2

Тема 5. Разработка модели комплексной системы защиты информации

Лабораторная работа 9

Название работы: Системный анализ информационной безопасности и принятие решения по ее защите от электромагнитных излучений и наводок

Время 1,5 часа

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Теоретическая часть

Все методы защиты от электромагнитных излучений и наводок можно разделить на пассивные и активные.

Пассивные методы обеспечивают уменьшение уровня опасного сигнала или снижение информативности сигналов.

Активные методы защиты направлены на создание помех в каналах побочных электромагнитных излучений и наводок, затрудняющих прием и выделение полезной информации из перехваченных злоумышленником сигналов.

Для блокирования угрозы воздействия на электронные блоки и магнитные запоминающие устройства мощными внешними

электромагнитными импульсами и высокочастотными излучениями, приводящими к неисправности электронных блоков и стирающими информацию с магнитных носителей информации, используется экранирование защищаемых средств.

Защита от побочных электромагнитных излучений и наводок осуществляется как пассивными, так и активными методами.

1. Пассивные методы защиты от побочных электромагнитных излучений и наводок

Пассивные методы защиты от ПЭМИН могут быть разбиты на три группы.

1.1. Экранирование

Экранирование является одним из самых эффективных методов защиты от ПЭМИН. Под экранированием понимается размещение элементов КС, создающих электрические, магнитные и электромагнитные поля, в заземленных, пространственно замкнутых конструкциях из токопроводящего материала. Обычно экраны изготавливаются из листовой стали или металлической сетки. В настоящее время в качестве экранов используются металлизированные ткани и металлические пленки, получаемые напылением на пластмассовых поверхностях и стекле.

Экранирование электрического поля заземленным экраном обеспечивается нейтрализацией электрических зарядов, стекающих по заземляющему контуру. Контур заземления должен иметь сопротивление не более 4 Ом.

Физические процессы, протекающие в экранах, зависят от частоты магнитного поля. Низкочастотные магнитные поля шунтируются экраном за счет направленности силовых линий вдоль стенок экрана. Этот эффект вызывается большей магнитной проницаемостью материала экрана по сравнению с воздухом. Высокочастотное магнитное поле вызывает возникновение переменных индукционных вихревых токов, которые создаваемым ими магнитным полем препятствуют распространению побочного магнитного поля. Заземление не влияет на экранирование магнитных полей. Поглощающая способность экрана зависит от частоты побочного излучения и от материала, из которого изготавливается экран. Чем ниже частота излучения, тем большей должна быть толщина экрана. Для излучений в диапазоне средних волн и выше достаточно эффективным

является экран толщиной 0,5 ~ 1,5 мм. Для излучений на частотах свыше 10 МГц достаточно иметь экран из меди или серебра толщиной 0,1 мм.

Электромагнитные излучения блокируются методами высокочастотного электрического и магнитного экранирования.

Экранирование осуществляется на пяти уровнях:

- ☐ уровень элементов схем;
- ☐ уровень блоков;
- ☐ уровень устройств;
- ☐ уровень кабельных линий; ☐ уровень помещений.

Элементы схем с высоким уровнем побочных излучений могут помещаться в металлические или металлизированные напылением заземленные корпуса. Начиная с уровня блоков, экранирование осуществляется с помощью конструкций из листовой стали, металлических сеток и напыления. Экранирование кабелей осуществляется с помощью металлической оплетки, стальных коробов или труб.

При экранировании помещений используются: листовая сталь толщиной до 2 мм, стальная (медная, латунная) сетка с ячейкой до 2,5 мм. В защищенных помещениях экранируются двери и окна. Окна экранируются сеткой, металлизированными шторами, металлизацией стекол и оклеиванием их токопроводящими пленками. Двери выполняются из стали или покрываются токопроводящими материалами (стальной лист, металлическая сетка). Особое внимание обращается на наличие электрического контакта токопроводящих слоев двери и стен по всему периметру дверного проема. При экранировании полей недопустимо наличие зазоров, щелей в экране. Размер ячейки сетки должен быть не более 0,1 длины волны излучения.

Выбор числа уровней и материалов экранирования осуществляется с учетом:

характеристик излучения (тип излучения, частота и мощность);
требований к уровню излучения за пределами контролируемой зоны и размеров зоны; наличия или отсутствия других методов защиты
от ПЭМИН; минимизации затрат на экранирование.

В защищенной ПЭНМ, например, экранируются блоки управления электронно-лучевой трубкой, корпус выполняется из стали или

металлизируется изнутри, экран покрывается металлической пленкой и (или) защищается металлической сеткой.

Экранирование, помимо выполнения своей прямой функции защиты от ПЭМИН, значительно снижает вредное воздействие электромагнитных излучений на организм человека. Экранирование позволяет также уменьшить влияние электромагнитных шумов на работу устройств.

1.2. Снижение мощности излучений и наводок

Способы защиты от ПЭМИН, объединенные в эту группу, реализуются с целью снижения уровня излучения и взаимного влияния элементов КС.

К данной группе относятся следующие методы:

- ☐ изменение электрических схем;
- ☐ использование оптических каналов связи;
- ☐ изменение конструкции;
- ☐ использование фильтров;
- ☐ гальваническая развязка в системе питания.

Изменения электрических схем осуществляются для уменьшения мощности побочных излучений. Это достигается за счет использования элементов с меньшим излучением, уменьшения крутизны фронтов сигналов, предотвращения возникновения паразитной генерации, нарушения регулярности повторений информации.

Перспективным направлением борьбы с ПЭМИН является использование оптических каналов связи. Для передачи информации на большие расстояния успешно используются волоконно-оптические кабели. Передачу информации в пределах одного помещения (даже больших размеров) можно осуществлять с помощью беспроводных систем, использующих излучения в инфракрасном диапазоне. Оптические каналы связи не порождают ПЭМИН. Они обеспечивают высокую скорость передачи и не подвержены воздействию электромагнитных помех.

Изменения конструкции сводятся к изменению взаимного расположения отдельных узлов, блоков, кабелей, сокращению длины шин.

Использование фильтров является одним из основных способов защиты от ПЭМИН. Фильтры устанавливаются как внутри устройств, систем для устранения распространения и возможного усиления наведенных побочных электромагнитных сигналов, так и на выходе из объектов линий связи, сигнализации и электропитания. Фильтры

рассчитываются таким образом, чтобы они обеспечивали снижение сигналов в диапазоне побочных наводок до безопасного уровня и не вносили существенных искажений полезного сигнала.

Полностью исключается попадание побочных наведенных сигналов во внешнюю цепь электропитания при наличии генераторов питания, которые обеспечивают гальваническую развязку между первичной и вторичной цепями.

Использование генераторов позволяет также подавать во вторичную цепь электропитание с другими параметрами по сравнению с первичной цепью. Так, во вторичной цепи может быть изменена частота по сравнению с первичной цепью. Генераторы питания, за счет инерционности, позволяют сглаживать пульсации напряжения и кратковременные отключения в первичной цепи.

1.3. Снижение информативности сигналов

Снижение информативности сигналов ПОМИН, затрудняющее их использование при перехвате, осуществляется следующими путями: ○ специальные схемные решения; ○ кодирование информации.

В качестве примеров специальных схемных решений можно привести такие, как замена последовательного кода параллельным, увеличение разрядности параллельных кодов, изменение очередности развертки строк на мониторе и т. п.

Для предотвращения утечки информации может использоваться кодирование информации, в том числе и криптографическое преобразование.

2. Активные методы защиты от ПЭМИН

Активные методы защиты от ПЭМИН предполагают использование генераторов шумов. В качестве маскирующих используются случайные помехи с нормальным законом распределения спектральной плотности мгновенных значений амплитуд (гауссовские помехи) и прицельные помехи, представляющие собой случайную последовательность сигналов помехи, идентичных побочным сигналам.

Используется пространственное и линейное зашумление. Пространственное зашумление осуществляется за счет излучения с помощью антенн электромагнитных сигналов в пространство. Применяется локальное пространственное зашумление для защиты конкретного элемента

КС и объективное пространственное зашумление для защиты от побочных электромагнитных излучений КС всего объекта. При локальном пространственном зашумлении используются прицельные помехи. Антенна находится рядом с защищаемым элементом КС. Объективное пространственное зашумление осуществляется, как правило, несколькими генераторами со своими антеннами, что позволяет создавать помехи во всех диапазонах побочных электромагнитных излучений всех излучающих устройств объекта.

При использовании линейного зашумления генераторы прицельных помех подключаются к линиям для создания в них электрических помех.

Пространственное зашумление должно обеспечивать невозможность выделения побочных излучений на фоне создаваемых помех во всех диапазонах излучения и, вместе с тем, уровень создаваемых помех не должен превышать санитарных норм и норм по электромагнитной совместимости радиоэлектронной аппаратуры.

Практическая часть

Задание:

1. Разработать классификацию методов и средств защиты компьютерной сети от электромагнитных излучений и наводок.
2. Предложить средства для защиты компьютерной сети объекта.

Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

Интернет-ресурсы: 1-3

Программное обеспечение: 1-2

Лабораторная работа 10

Название работы: Системный анализ информационной безопасности и принятие решения по ее защите от несанкционированного изменения структур
Время 1,5 часа

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Теоретическая часть

Общие требования к защищенности КС от несанкционированного изменения структур

Несанкционированному изменению могут быть подвергнуты алгоритмическая, программная и техническая структуры КС на этапах ее разработки и эксплуатации. На этапе эксплуатации необходимо выделить работы по модернизации КС, представляющие повышенную опасность для безопасности информации.

Особенностью защиты от несанкционированного изменения структур (НИС) КС является универсальность методов, позволяющих наряду с умышленными воздействиями выявлять и блокировать непреднамеренные ошибки разработчиков и обслуживающего персонала, а также сбои и отказы аппаратных и программных средств. Обычно НИС КС, выполненные на этапе разработки и при модернизации системы, называют закладками.

Для парирования угроз данного класса на различных этапах жизненного цикла КС решаются различные задачи. На этапе разработки и при модернизации КС основной задачей является исключение ошибок и возможности внедрения закладок. На этапе эксплуатации выявляются закладки и ошибки, а также обеспечивается целостность, неизменность структур.

Разработке программных и аппаратных средств предшествует разработка алгоритмов. Ошибки и закладки, внесенные и не устраненные на этапе разработки алгоритмов, переходят в программы и оборудование, если не будут своевременно обнаружены.

При разработке алгоритмов, программ и аппаратных средств необходимо придерживаться основных принципов, которые являются общими:

- привлечение к разработке высококвалифицированных специалистов;

- ☐ использование иерархических структур;
- ☐ применение стандартных блоков;
- ☐ дублирование разработки;
- ☐ контроль адекватности;
- ☐ многослойная фильтрация; ☐ автоматизация разработки; ☐ контроль процесса разработки; ☐ сертификация готового продукта.

Особые требования к квалификации предъявляются к специалистам, занятым разработкой технического задания, алгоритмов и осуществляющих контроль за ходом разработки, а также специалистов, привлекаемых к сертификации готовых продуктов.

Представление любой системы в виде иерархической блочной структуры позволяет представлять любой блок в виде черного ящика. Блочная структура системы позволяет упростить контроль функционирования системы, использовать стандартные отлаженные и проверенные блоки, допускает параллельную разработку всех блоков и дублирование разработки.

Под дублированием разработки алгоритма программы или устройства понимается независимая (возможно разными организациями) разработка одного и того же блока. Сравнение блоков позволяет, во-первых, выявить ошибки и закладки, а во-вторых, выбрать наиболее эффективный блок.

Проверка адекватности функционирования алгоритма, программы, устройства реализуется путем моделирования процессов, использования упрощенных (усеченных) алгоритмов, решения обратной задачи (если она существует), а также с помощью тестирования. Тестирование является универсальным средством проверки, как адекватности, так и работоспособности блоков. Если число входных воздействий и внешних условий конечно и может быть задано при испытании блока за приемлемое для практики время, а также известны все требуемые реакции блока, то адекватность функционирования блока может быть однозначно подтверждена, т. е. в блоке полностью отсутствуют ошибки и закладки. Обнаружение ошибок и закладок тестированием осложняется тем, что мощность входного множества по оценкам специалистов может достигать $10^{70} - 10^{100}$. Поэтому для тестирования по всей области входных воздействий потребуется практически бесконечное время. В таких случаях

используется вероятностный подход к выборке входных воздействий. Но такая проверка не может гарантировать отсутствия закладок и ошибок.

Принцип многослойной "фильтрации" предполагает поэтапное выявление ошибок и закладок определенного класса. Например, могут использоваться "фильтрующие" программные средства для выявления возможных "временных", "интервальных", "частотных" и других типов закладок.

Автоматизация процесса разработки существенно снижает возможности внедрения закладок. Это объясняется, прежде всего, наличием большого числа типовых решений, которые исполнитель изменить не может, формализованностью процесса разработки, возможностью автоматизированного контроля принимаемых решений.

Контроль установленного порядка разработки предполагает регулярный контроль за действиями исполнителей, поэтапный контроль алгоритмов, программ и устройств, приемо-сдаточные испытания.

Разработка защищенных КС и элементов для них завершается сертификацией готового продукта. Сертификация проводится в специальных лабораториях, оснащенных испытательными стендами, укомплектованных специалистами соответствующей квалификации и имеющих официальное разрешение (лицензию) на такой вид деятельности. В таких лабораториях по определенным методикам осуществляется проверка программных и аппаратных средств на отсутствие закладок, а также соответствие средств защиты информации их назначению.

Практическая часть

Контрольно-испытательный стенд должен обеспечивать всесторонний анализ испытуемого программного средства в условиях, максимально приближенных к тем, в которых оно будет использоваться в реальной системе. Испытание проводится путем многократной подачи входных воздействий на фоне изменяющихся внешних факторов, с помощью которых имитируется воздействие возможных закладок. Таким образом, контрольно-испытательный стенд может рассматриваться как детальная имитационная модель разрабатываемой системы, позволяющая обеспечить всесторонний анализ функционирования разрабатываемого программного средства в условиях воздействия закладок.

Задание:

1. Провести системный анализ существующих методов защиты от несанкционированного изменения структуры КС.

1. Разработать требования к контрольно-испытательному стенду для обнаружения закладок и ошибок в разрабатываемых программных средствах.

2. Разработать структурную схему контрольно-испытательного стенда.

Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

Интернет-ресурсы: 1-3

Программное обеспечение: 1-2

Тема 6. Технологическое и организационное построение комплексной системы защиты информации

Лабораторная работа 11

Название работы: Системный анализ информационной безопасности и принятие решения по ее защите от несанкционированного доступа в компьютерную сеть

Время 1,5 часа

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Теоретическая часть

Для осуществления НСДИ злоумышленник не применяет никаких аппаратных или программных средств, не входящих в состав КС. Он осуществляет НСДИ, используя:

- знания о КС и умения работать с ней;
- сведения о системе защиты информации;
- сбои, отказы технических и программных средств;
- ошибки, небрежность обслуживающего персонала и пользователей.

Для защиты информации от НСД создается система разграничения доступа (СРД) к информации. Получить несанкционированный доступ к информации при наличии системы разграничения доступа возможно только при сбоях и отказах КС, а также используя слабые места в комплексной системе защиты. Чтобы использовать слабости в системе защиты, злоумышленник должен знать о них. Одним из путей добывания информации о недостатках системы защиты является изучение механизмов защиты. Злоумышленник может тестировать систему защиты путем непосредственного контакта с ней. В этом случае велика вероятность обнаружения системной защиты попыток ее тестирования. В результате этого службой могут быть предприняты дополнительные меры защиты. Гораздо более привлекательным для злоумышленника является другой подход. Сначала получается копия программного средства системы защиты или техническое средство защиты, а затем производится их исследование в лабораторных условиях. Кроме того, создание неучтенных копий на съемных носителях информации является одной из распространенных и

удобных способов хищения информации. Этим способом осуществляется несанкционированное тестирование программ. Скрыто получить технические средства защиты для исследования гораздо сложнее, чем программное, и такая угроза блокируется средствами и методами обеспечения целостности технической структуры КС.

Для блокирования несанкционированного исследования и копирования информации КС используется комплекс средств и мер защиты, которые объединяются в систему защиты от исследования и копирования информации (СЗИК).

Таким образом, СРД и СЗИК могут рассматриваться как подсистемы защиты от НСДИ.

Практическая часть

Задание:

1. Разработать состав системы разграничения доступа (СРД).
2. Представить структурную схему диспетчера доступа.
3. На основе анализа комплекса методов и средств защиты от несанкционированного исследования и копирования информации КС разработать СЗИК.

Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

Интернет-ресурсы: 1-3

Программное обеспечение: 1-2

Лабораторная работа № 12

Название работы: Системный анализ информационной безопасности и принятие решения по ее защите криптографическими методами

Время 1,5 часа

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Цели:

- изучить основные подходы к защите информационной системы организации криптографическими методами;
- выработать навыки проведения исследования комплексной системы защиты информации на предмет выявления угроз безопасности и разработки предложений по использованию криптографической защиты.

Требования квалификационной характеристики:

уметь применять на практике существующие подходы к обеспечению безопасности информационного ресурса организации.

Учебно-материальное обеспечение: технические средства обучения (ПЭВМ).

Прежде чем приступить к выполнению заданий, необходимо ответить на следующие вопросы:

1. Определение понятия «информационная система».
2. Компоненты информационной системы.
3. Определение понятий «анализ» и «синтез».
4. Распространенные угрозы информационной системе организации.
5. Аппаратные средства, ориентированные на защиту информационной системы организации.
6. Программные средства, ориентированные на защиту информационной системы организации.
7. Методы защиты информационной системы организации.
8. Технологии, используемые в комплексной системе защиты информации для защиты информационной системы организации.
9. Определение понятия «криптографических методов защиты».
10. Примеры алгоритмов защиты информации с помощью криптографических методов.

11. Приведите классификацию методов криптографического преобразования информации и поясните сущность методов.
12. Назовите и охарактеризуйте методы шифрования.
13. Сравните наиболее распространенные стандарты шифрования.
14. Каковы перспективы криптозащиты информации в КС?
15. Алгоритм RSA.

Теоретическая часть

Защита информации методами криптографического преобразования заключается в изменении ее составных частей (слов, букв, слогов, цифр) с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, то есть в приведении ее к неявному виду. Для ознакомления с шифрованной информацией применяется обратный процесс: декодирование (дешифрование). Использование криптографии является одним из распространенных методов, значительно повышающих безопасность передачи данных в сетях ЭВМ, данных, хранящихся в удаленных устройствах памяти, а также при обмене информацией между удаленными объектами.

Для преобразования (шифрования) обычно используются некоторый алгоритм или устройство, реализующее заданный алгоритм, который может быть известен широкому кругу лиц. Управление процессом шифрования осуществляется с помощью периодически меняющегося кода ключа, обеспечивающего каждый раз оригинальное представление информации при использовании одного и того же алгоритма или устройства. Знание ключа позволяет просто и надежно расшифровать текст. Однако без знания ключа эта процедура может быть практически невыполнима даже при известном алгоритме шифрования. Даже простое преобразование информации является весьма эффективным средством, дающим возможность скрыть ее смысл от большинства неквалифицированных нарушителей.

Алгоритмы шифрования предназначены для решения задачи обеспечения конфиденциальности информации. В настоящее время для закрытия информации интенсивно используются криптографические методы. С древнейших времен наиболее эффективной формой защиты было

и остается шифрование. Шифрование определяется как взаимнообратное преобразование незащищенной (открытой) информации в зашифрованную (закрытую) форму – шифртекст, в которой она не представлена полностью доступной для злоумышленника. При шифровании используются ключи, наличие которых означает возможность зашифрования и/или расшифрования информации. Важно отметить, что сам метод шифрования не требуется держать в секрете, т.к. знание только его не позволит расшифровать шифртекст. Современные криптосистемы можно однозначно разделить по способу использования ключей на криптосистемы с секретным ключом (симметричные) и с открытым ключом (асимметричные). Если для зашифрования и расшифрования используется один и тот же ключ, такая криптосистема называется симметричной.

К симметричным криптосистемам относятся DES, AES, ГОСТ 2814789 и т.д. Новым направлением в криптографии стало изобретение асимметричных криптосистем с открытым ключом, таких, как RSA, DSA или Эль-Гамаль.

В асимметричных криптосистемах для зашифрования и расшифрования применяют различные, практически не выводимые друг из друга ключи, один из которых (ключ расшифрования) делается секретным, а другой (ключ зашифрования) – открытым. Этим достигается возможность передавать секретные сообщения по незащищенному каналу без предварительной передачи секретного ключа. Именно криптография с открытым ключом разорвала порочный круг симметричных шифров, когда для организации обмена секретной информацией надо было сначала произвести распределение секретных ключей.

Алгоритм шифрования считается стойким, если, имея закрытые данные, и зная секретный ключ, невозможно получить информацию об открытых данных. Строго доказана невозможность построения абсолютно стойкого шифра, за исключением случая, когда размер секретного ключа равен (или больше) размеру шифруемых данных. Этот случай трудно реализуем на практике, т.к. реально применяемые и доступные на рынке средства криптографической защиты используют шифры, для которых задача восстановления открытого текста по закрытому является трудно вычислимой, то есть требует настолько больших ресурсов, что атака становится экономически нецелесообразной.

Среди симметричных шифров наиболее известны и часто используются следующие (размер блока в битах обозначен как b , число циклов через r , а длина ключа – l):

- DES – государственный стандарт США ($b = 64$, $r = 16$, $l = 56$). В настоящее время доказана недостаточная стойкость DES против атаки методом простого перебора;

– Triple DES и DESX ($b = 64$, $r = 16$, $l = 168; 112$) – последовательное применение алгоритма DES с разными ключами, что обеспечивает значительную устойчивость к взлому;

– IDEA – ($b = 64$, $r = 8$, $l = 128$). Активные исследования его стойкости выявили в нем ряд слабых ключей, однако вероятность их использования пренебрежимо мала;

– RC5 – параметризованный шифр;

– ГОСТ 28147 – российский стандарт шифрования данных ($b = 64$, $r = 32$, $l = 256$). Для ГОСТа было найдено множество слабых ключей, значительно снижающих его эффективную стойкость в простых режимах шифрования. В то же время доказано, что высока вероятность получения слабых узлов замены, упрощающих криптоанализ данного шифра;

– Blowfish – это 64-битовый блочный шифр, разработанный Шнайером (Schneier) в 1993 г., реализуется посредством перестановок и замен, зависящих от ключа.

В мире разработано, опубликовано и исследовано достаточно большое число симметричных алгоритмов, из которых лишь DES и его модификация Triple DES были достаточно проверены временем.

Криптосистемы с открытым ключом строятся, как правило, на основе сложной математической задачи вычисления функции, обратной заданной. Такие функции называются однонаправленными, т.е. их обращение представляет собой практически неразрешимую задачу. Суть метода шифрования в том, что вычисление функции от зашифрованного сообщения в прямом направлении проходит с использованием открытого ключа принимающего абонента, а при расшифровке (вычислении обратной функции) применяется его секретный ключ. Как и следовало ожидать, математических задач, удовлетворяющих перечисленным требованиям, известно немного, и лишь на некоторых из них были построены используемые на практике шифры. Наиболее известные криптосистемы с открытым ключом:

– RSA. Используется задача факторизации (вычисления простых сомножителей) большого целого числа. Построен на основе перемножения двух простых чисел большой разрядности. Широко применяется в криптографических протоколах закрытия информации и аутентификации;

—

— Эль-Гамаль (El-Gamal). Основан на задаче дискретного логарифмирования в конечном поле. Используется в стандартах электронной цифровой подписи (ЭЦП) DSS, ГОСТ Р34.10 и т.д.; Эллиптические кривые (elliptic curve). Основан на задаче дискретного логарифмирования на эллиптических кривых в конечном поле. Криптосистемы с открытым ключом используются в основном в трех направлениях:

- закрытие информации;
- аутентификация с использованием ЭЦП;
- защищенное от перехвата распределение открытых ключей.

Практическая часть

Провести анализ комплексной системы защиты информации конкретной организации с выявлением проблем защиты информации в информационной системе. Представить структуру комплексной системы защиты информации, включающей в себя расположение ее компонент в помещениях организации с обозначением отделов. Разработать классификации:

- угроз информационной системы организации;
- используемых и предлагаемых методов защиты информационного ресурса организации;
- используемых и предлагаемых технологий на базе комплексной системы защиты информации, ориентированных на защиту информационной системы.

Разработать процедуру принятия решений по нейтрализации выявленных проблем, включающей в себя следующие этапы:

- формулировка проблемной ситуации;
- определение целей;
- определение критериев достижения целей;
- построение моделей для обоснования решений;
- поиск оптимального (допустимого) варианта решения;
- согласование решения;
- подготовка решения к реализации;

-
- утверждение решения;
- управление ходом реализации решения; —
- проверка эффективности решения.

Отчет по результатам выполненной лабораторной работы должен содержать:

характеристику организации, включая бизнес-процессы, количество штатных единиц персонала, годовой объем выручки и организационную структуру;

- схему комплексной системы защиты информации организации с описанием компонент;

- классификации угроз, используемых и предлагаемых методов и технологий для защиты информационной системы организации;

- процедуру принятия решений по нейтрализации выявленных проблем в защите информационной системы организации, включающей в себя количественные оценки эффективности комплексной системы защиты информации.

Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

Интернет-ресурсы: 1-3

Программное обеспечение: 1-2

Тема 7. Назначение, структура и содержание управления комплексной системы защиты информации

Лабораторная работа 13

Название работы: Системный анализ информационной безопасности и принятие решения по ее защите от компьютерных вирусов

Время 4,5 часа

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Цели:

- изучить основные подходы к защите информационной системы организации криптографическими методами;
- выработать навыки проведения исследования комплексной системы защиты информации на предмет выявления угроз безопасности и разработки предложений по использованию криптографической защиты.

Требования квалификационной характеристики:

уметь применять на практике существующие подходы к обеспечению безопасности информационного ресурса организации.

Учебно-материальное обеспечение:

технические средства обучения (ПЭВМ).

Теоретическая часть

В настоящее время очевидно смещение вектора компьютерных атак от массового заражения к целевым, точечным атакам. Как сказал Е. Касперский: «Девяностые были десятилетием киберхулиганов, двухтысячные были десятилетием киберпреступников, сейчас наступила эра кибервойн и кибертеррора». Иллюстрацией этому являются всем известные примеры: Stuxnet, Duqu, Flamer, Gauss, которые многие антивирусные компании причисляют к кибероружию.

Одним из ярких примеров использования кибероружия может служить шпионская сеть «Красный октябрь», которая пять лет активно добывала информацию из правительственных организаций, различных исследовательских институтов, крупных международных компаний. Серьезная защищенность этих объектов не остановила работу вредоносной

системы. Она была раскрыта всего несколько месяцев назад, что свидетельствует о возрастающей угрозе вмешательства в работу любой компьютерной системы.

Для обеспечения устойчивого и неопределяемого присутствия в компьютерной системе вредоносное программное обеспечение (ВПО) использует специальные механизмы, называемые руткит-механизмами. В результате ВПО работает незаметно как для пользователя, так и для средств защиты.

Казалось бы, разработчики ОС должны всеми силами противостоять сокрытию нелегитимного ПО, однако появление новой версии Windows не изменило ситуацию в лучшую сторону. "Восьмерка" переняла от своих предшественников часть уже знакомых механизмов защиты (UAC, ASLR, DEP, PatchGuard, цифровые подписи для драйверов), для которых существует возможность обхода. И представила несколько новых — Secure Boot, SMEP и ELAM, которые, однако, не сильно повысили уровень защищенности. О чем свидетельствуют демообразец буткита Stoned Lite Питера Кляйсснера и EFI bootkit Андреа Аллиеви. А о возможности обхода технологии SMEP на Windows 8 уже писал А. Шишкин из компании Positive Technologies.

Согласно недавнему отчету британской Национальной аудиторской службы (NAO), наблюдается рост числа киберпреступлений, которые одной Великобритании обходятся в 18–27 миллиардов фунтов стерлингов ежегодно.

Исходя из сказанного, можно сделать вывод, что в последней версии Windows для борьбы с ВПО ничего революционно нового не было внедрено, и достойных механизмов, способных сильно осложнить жизнь разработчикам руткитов, на сегодняшний момент нет.

Для сокрытия ВПО могут применяться различные методы. Впервые классификация механизмов сокрытия была выполнена Йоанной Рутковской в работе *Introducing Stealth Malware Taxonomy*. Предложенная ей классификация может быть расширена следующим образом (рисунок 13.1).



Рисунок 13.1 - Классификаций руткит-технологий

Стеганографические механизмы скрывают истинное предназначение внедренных объектов маскировкой их под легитимные, например схожестью их имен с именами системных файлов. В результате вредоносные файлы видны пользователю, но не вызывают у него подозрения. Пример стеганографического сокрытия — использование сертификатов доверенных компаний для подписи вредоносных драйверов. Благодаря действительным сертификатам компаний Realtek и JMicron червь Stuxnet долгое время оставался незамеченным, а компоненты червя Flame имели цифровую подпись самой компании Microsoft.

Для работы стеганографических механизмов не требуется повышенных привилегий, также они переносятся на различные версии ОС Windows. Однако из-за отсутствия технических механизмов сокрытия такое ВПО может быть легко обнаружено и удалено. Большую опасность представляют комбинации стеганографических с другими механизмами сокрытия.

Ко второй группе относятся технические механизмы сокрытия, в результате работы которых информация о скрываемом объекте становится недоступной средству обнаружения («не виден объект, значит, его и нет»). Эти механизмы можно разделить на руткит-механизмы, работающие «внутри» и «вне» ОС.

В случае руткит-механизма «внутри ОС» объектом может выступать процесс, драйвер, файл на диске, сетевой порт, ключ в реестре. Для своей работы руткит-механизмы могут изменять как пути выполнения, так и

структуры памяти, как в пользовательском, так и в системном адресных пространствах.

Для изменения пути выполнения ВПО перехватывает функции штатного обработчика и передает управление вредоносному обработчику, который вносит целенаправленные изменения в возвращаемый результат. Способы обнаружения описанного механизма сокрытия уже освещались на страницах журнала.

Вторая подгруппа руткит-механизмов, работающих «внутри» ОС, не добавляет новых обработчиков в систему, а особым образом изменяет структуры памяти, хранящие информацию о скрываемом объекте. Примеры таких структур, расположенных в системном адресном пространстве и представляющих интерес для руткитов: KRPCB, ETHREAD, EPROCESS, MODULE_ENTRY, _DRIVER_OBJECT, плюс БД зарегистрированных драйверов и служб, расположенная в пользовательском пространстве процесса SERVICES.EXE.

Руткит-механизмы «вне ОС» основаны на установке собственного или модификации существующего обработчика событий в том или ином режиме работы процессора либо дополнительного аппаратного обеспечения. Для работы этих механизмов зачастую необходимо наличие набора микросхем с поддержкой требуемой технологии. Можно выделить руткит-механизмы, построенные на основе режима аппаратной виртуализации, режима системного управления и кода, использующего технологии Active Management Technology и V-PRO. Широко известный в узких кругах автор R_T_T в своих работах «Кремневый беспредел» описывает возможности и угрозы информационной безопасности не только от указанных технологий, но и от механизма обновления микрокода процессора (bit.ly/VRQD6O и bit.ly/104EsRB).

На конференции ZeroNight в 2012 году была представлена работа Д. Олексюка (Cr4sh) в которой описывался интересный способ размещения руткита не в файлах, а в реестре с помощью Differentiated System Description Table (DSDT). Преимущество данного способа в том, что ни одно средство для обнаружения руткитов не учитывает такую возможность.

Современные тенденции развития средств антивирусной защиты

Антивирусная программа (антивирус) — специализированная программа для обнаружения компьютерных вирусов, а также

нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Классифицировать антивирусные продукты можно сразу по нескольким признакам, таким, как: используемые технологии антивирусной защиты, функционал продуктов, целевые платформы.

По используемым технологиям антивирусной защиты:

1. Классические антивирусные продукты (продукты, применяющие только сигнатурный метод детектирования)
2. Продукты проактивной антивирусной защиты (продукты, применяющие только проактивные технологии антивирусной защиты);
3. Комбинированные продукты (продукты, применяющие как классические, сигнатурные методы защиты, так и проактивные) По функционалу продуктов:

1. Антивирусные продукты (продукты, обеспечивающие только антивирусную защиту)
2. Комбинированные продукты (продукты, обеспечивающие не только защиту от вредоносных программ, но и фильтрацию спама, шифрование и резервное копирование данных и другие функции) По целевым платформам:

1. Антивирусные продукты для ОС семейства Windows
2. Антивирусные продукты для ОС семейства *NIX (к данному семейству относятся ОС BSD, Linux и др.)
3. Антивирусные продукты для ОС семейства MacOS
4. Антивирусные продукты для мобильных платформ (Windows Mobile, Symbian, iOS, BlackBerry, Android, Windows Phone и др.)

Антивирусные продукты для корпоративных пользователей можно также классифицировать по объектам защиты:

1. Антивирусные продукты для защиты рабочих станций
2. Антивирусные продукты для защиты файловых и терминальных серверов

3. Антивирусные продукты для защиты почтовых и Интернет-шлюзов 4. Антивирусные продукты для защиты серверов виртуализации

Обнаружение, основанное на сигнатурах — метод работы антивирусов и систем обнаружения вторжений, при котором программа, просматривая файл или пакет, обращается к словарю с известными вирусами, составленному авторами программы. В случае соответствия какого-либо участка кода просматриваемой программы известному коду (сигнатуре) вируса в словаре, программа антивирус может заняться выполнением одного из следующих действий:

- ☐ Удалить инфицированный файл.
- ☐ Отправить файл в «карантин» (то есть сделать его недоступным для выполнения, с целью недопущения дальнейшего распространения вируса).
- ☐ Попытаться восстановить файл, удалив сам вирус из тела файла.

Для достижения достаточно продолжительного успеха при использовании этого метода необходимо периодически пополнять словарь известных вирусов новыми определениями (в основном в онлайн-режиме). Обладающие чувством гражданского долга и технически искушённые пользователи, обнаружив «живьём» новый вирус, могут выслать заражённый файл разработчикам антивирусных программ, которые включат затем новый вирус в словарь.

Антивирусные программы, созданные на основе метода соответствия определению вирусов в словаре, обычно просматривают файлы тогда, когда компьютерная система создаёт, открывает, закрывает или посылает файлы по электронной почте. Таким образом, вирусы можно обнаружить сразу же после занесения их в компьютер и до того, как они смогут причинить какой-либо вред. Надо отметить, что системный администратор может составить график для антивирусной программы, согласно которому могут просматриваться (сканироваться) все файлы на жёстком диске.

Хотя антивирусные программы, созданные на основе поиска соответствия определению вируса в словаре, при обычных обстоятельствах могут достаточно эффективно препятствовать вспышкам заражения компьютеров, авторы вирусов стараются держаться на полшага впереди

таких программ-антивирусов, создавая «олигоморфические», «полиморфические» и самые новые «метаморфические» вирусы, в которых некоторые части участки кода перезаписываются, модифицируются, шифруются или искажаются так, чтобы невозможно было обнаружить совпадение с определением в словаре вирусов.

Сигнатуры антивирусов создаются в результате кропотливого анализа нескольких копий файла, принадлежащего одному вирусу. Сигнатура должна содержать только уникальные строки из этого файла, настолько характерные, чтобы гарантировать минимальную возможность ложного срабатывания — главный приоритет любой антивирусной компании.

Разработка сигнатур — ручной процесс, тяжело поддающийся автоматизации. Несмотря на массу исследований, посвящённых автоматической генерации сигнатур, нарастающий полиморфизм (и «метаморфизм») вирусов и атак делают синтаксические сигнатуры бессмысленными.

Достоинство синтаксических сигнатур: позволяют определять конкретную атаку с высокой точностью и малой долей ложных вызовов
Недостатки:

- Беззащитны перед полиморфными вирусами и изменёнными версиями того же вируса;
- Требуют регулярного и крайне оперативного обновления; ○
Требуют кропотливого ручного анализа вирусов;
- Неспособны выявить какие-либо новые атаки.

Проактивные технологии — совокупность технологий и методов, используемых в антивирусном программном обеспечении, основной целью которых, в отличие от реактивных (сигнатурных) технологий, является предотвращение заражения системы пользователя, а не поиск уже известного вредоносного программного обеспечения в системе. При этом проактивная защита старается блокировать потенциально опасную активность программы только в том случае, если эта активность представляет реальную угрозу. Серьезный недостаток проактивной защиты - блокирование легитимных программ.

Технологии проактивной защиты

1. Эвристический анализ

Технология эвристического анализа позволяет на основе анализа кода выполняемого приложения, скрипта или макроса обнаружить участки кода, отвечающие за вредоносную активность.

Эффективность данной технологии не является высокой, что обусловлено большим количеством ложных срабатываний при повышении чувствительности анализатора, а также большим набором техник, используемых авторами вредоносного ПО для обхода эвристического компонента антивирусного ПО.

2. Эмуляция кода

Технология эмуляции позволяет запускать приложение в среде эмуляции, эмулируя поведение ОС или центрального процессора. При выполнении приложения в режиме эмуляции приложение не сможет нанести вреда системе пользователя, а вредоносное действие будет детектировано эмулятором.

Несмотря на кажущуюся эффективность данного подхода, он также не лишен недостатков – эмуляция занимает слишком много времени и ресурсов компьютера пользователя, что негативно сказывается на быстродействии при выполнении повседневных операций, также, современные вредоносные программы способны обнаруживать выполнение в эмулированной среде и прекращать свое выполнение в ней.

3. Анализ поведения

Технология анализа поведения основывается на перехвате всех важных системных функций или установке т.н. мини-фильтров, что позволяет отслеживать всю активность в системе пользователя. Технология поведенческого анализа позволяет оценивать не только единичное действие, но и цепочку действий, что многократно повышает эффективность противодействия вирусным угрозам. Также, поведенческий анализ является технологической основой для целого класса программ – поведенческих блокираторов (HIPS – Host-based Intrusion Systems).

4. Sandboxing (Песочница) – ограничение привилегий выполнения

Технология Песочницы работает по принципу ограничения активности потенциально вредоносных приложений таким образом, чтобы они не могли нанести вреда системе пользователя.

Ограничение активности достигается за счет выполнения неизвестных приложений в ограниченной среде – собственно песочнице, откуда

приложение не имеет прав доступа к критическим системным файлам, веткам реестра и другой важной информации. Технология ограничения привилегий выполнения является эффективной технологией противодействия современным угрозам, но, следует понимать, что пользователь должен обладать знаниями, необходимыми для правильной оценки неизвестного приложения.

5. Виртуализация рабочего окружения

Технология виртуализации рабочего окружения работает с помощью системного драйвера, который перехватывает все запросы на запись на жесткий диск и вместо выполнения записи на реальный жесткий диск выполняет запись в специальную дисковую область – буфер. Таким образом, даже в том случае, если пользователь запустит вредоносное программное обеспечение, оно проживет не далее чем до очистки буфера, которая по умолчанию выполняется при выключении компьютера.

Однако, следует понимать, что технология виртуализации рабочего окружения не сможет защитить от вредоносных программ, основной целью которых является кража конфиденциальной информации, т.к. доступ на чтение к жесткому диску не запрещен.

Кроме того, последние годы крупные компании склоняются к использованию централизованных аппаратно-программных комплексов, защищающих внутреннюю сеть предприятия от вирусной угрозы. К таким решениям относятся в том числе и программно-аппаратные руткиты на основе технологий виртуализации.

Практическая часть

Провести анализ комплексной системы защиты информации конкретной организации с выявлением проблем защиты информации от вирусных угроз. Определить узлы компьютерной сети предприятия, наиболее чувствительные для вирусной угрозы. Провести анализ эффективности программных антивирусных продуктов и разработать рекомендации по использованию средств антивирусной защиты информации в корпоративной сети предприятия.

Отчет по результатам выполненной лабораторной работы должен содержать:

- характеристику организации, включая бизнес-процессы, количество штатных единиц персонала, годовой объем выручки и организационную структуру;
- схему компьютерной сети предприятия с выделенными узлами, чувствительными к вирусной угрозе;
- классификацию вирусных угроз, используемых и предлагаемых методов и технологий для защиты информации в сети предприятия;
- обоснование выбора того или иного продукта для использования в качестве средства защиты от вирусной угрозы (преимущества);
- процедуру принятия решений по нейтрализации выявленных проблем в защите от вирусов информационной системы организации.

Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

Интернет-ресурсы: 1-3

Программное обеспечение: 1-2

Лабораторная работа 14

Название работы: Системный анализ информационной безопасности и принятие решения по ее защите в распределенных компьютерных сетях

Время 4,5 часа

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Теоретическая часть

1. Архитектура распределенных компьютерных систем

Под распределенными понимаются КС, которые не располагаются на одной контролируемой территории, на одном объекте. В общем случае распределенная компьютерная система (РКС) представляет собой множество сосредоточенных КС, связанных в единую систему с помощью коммуникационной подсистемы. Сосредоточенными КС могут быть отдельные ЭВМ, в том числе и ПЭВМ, вычислительные системы и

комплексы, а также ЛВС. В настоящее время практически не используются неинтеллектуальные абонентские пункты, не имеющие в своем составе ЭВМ. Поэтому правомочно считать, что наименьшей структурной единицей РКС является ЭВМ. Распределенные КС строятся по сетевым технологиям и представляют собой вычислительные сети (ВС). Коммуникационная подсистема включает в себя коммуникационные модули (КМ), связанные высокоскоростными каналами связи, концентраторы для уплотнения информации перед передачей ее по высокоскоростным каналам, межсетевые шлюзы (мосты) для связи сети с ЛВС или для связи сегментов глобальных сетей. С помощью мостов связываются сегменты сети с одинаковыми сетевыми протоколами. Основной функцией коммуникационных модулей является передача полученного пакета к другому КМ или абонентскому пункту в соответствии с маршрутом передачи. Коммуникационный модуль называют также центром коммутации пакетов или маршрутизатором.

В любой РКС в соответствии с функциональным назначением может быть выделено три подсистемы:

- пользовательская подсистема; - подсистема управления;
- коммуникационная подсистема.

Пользовательская или абонентская подсистема включает в себя компьютерные системы пользователей (абонентов) и предназначена для удовлетворения потребностей пользователей в хранении, обработке и получении информации.

Наличие подсистемы управления позволяет объединить все элементы РКС в единую систему, в которой взаимодействие элементов осуществляется по единым правилам. Подсистема обеспечивает взаимодействие элементов системы путем сбора и анализа служебной информации и воздействия на элементы с целью создания оптимальных условий для функционирования всей сети.

Коммуникационная подсистема обеспечивает передачу информации в сети в интересах пользователей и подсистемы управления.

Функционирование РКС можно рассматривать как взаимодействие удаленных процессов через коммуникационную подсистему. Процессы вычислительной сети порождаются пользователями (абонентами) и

другими процессами. Взаимодействие удаленных процессов заключается в обмене файлами, пересылке сообщений по электронной почте, посылке заявок на выполнение программ и получение результатов, обращении с запросами к базам данных и т. д.

2. Особенности защиты информации в РКС

С точки зрения защиты информации в РКС важно разделить ВС на корпоративные и общедоступные. В корпоративных сетях все элементы принадлежат одному ведомству, за исключением, может быть, каналов связи. В таких сетях имеется возможность проводить единую политику обеспечения безопасности информации во всей сети. Примерами таких корпоративных сетей могут служить сети государственного и военного управления, сети авиационных и железнодорожных компаний и др. Противоположностью таким сетям являются общедоступные коммерческие сети, в которых во главу угла ставится распространение информации, а вопросы защиты собственных информационных ресурсов решаются, в основном, на уровне пользователей. В качестве примера такой сети можно привести сеть Internet. Корпоративные сети могут быть связаны с общедоступными сетями. В этом случае администрации (владельцам) корпоративных сетей необходимо предпринимать дополнительные меры предосторожности для блокирования возможных угроз со стороны общедоступных сетей.

При построении системы защиты информации в любой РКС необходимо учитывать:

- сложность системы, которая определяется как количеством подсистем, так и разнообразием их типов и выполняемых функций;
- невозможность обеспечения эффективного контроля за доступом к ресурсам, распределенным на больших расстояниях, возможно за пределами границ страны;
- возможность принадлежности ресурсов сети различным владельцам.

Особенностью защиты информации от непреднамеренных угроз в РКС по сравнению с сосредоточенными сетями является необходимость обеспечения гарантированной передачи информации по коммуникационной подсети. Для этого в РКС должны быть предусмотрены дублирующие маршруты доставки сообщений, предприняты меры против

искажения и потери информации в каналах связи. Такие сложные системы должны строиться как адаптивные, в которых обеспечивается постоянный контроль работоспособности элементов системы и возможность продолжения функционирования даже в условиях отказов отдельных подсистем. Искажения информации в каналах связи фиксируются и частично исправляются с помощью помехоустойчивого кодирования. Потери информации исключаются за счет использования контроля и учета принятых сообщений, а также за счет применения протоколов обмена с подтверждением о приеме информации.

В РКС все потенциальные преднамеренные угрозы безопасности информации обычно делят на две группы угроз: пассивные и активные.

К пассивным относятся угрозы, целью реализации которых является получение информации о системе путем прослушивания каналов связи. Подключившись к каналам связи или являясь пользователем системы, злоумышленник может:

- получить информацию путем перехвата незашифрованных сообщений;

- анализировать трафик (поток сообщений), накапливая информацию об интенсивности обмена отдельных абонентов, о структуре сообщений, о маршрутах доставки сообщений и т. п.

Активные угрозы предусматривают воздействие на передаваемые сообщения в сети и несанкционированную передачу фальсифицированных сообщений с целью воздействия на информационные ресурсы объектов РКС и дестабилизацию функционирования системы. Возможно также непосредственное воздействие на коммуникационную подсистему с целью повреждения аппаратных средств передачи информации.

Передаваемые в РКС сообщения могут несанкционированно модифицироваться или уничтожаться. Злоумышленник может размножать перехваченные сообщения, нарушать их очередность следования, изменять маршрут доставки, подменять сообщения. Злоумышленник может предпринять попытки несанкционированного доступа к информационным ресурсам удаленного объекта КС, осуществления несанкционированного изменения программной структуры КС путем внедрения вредительских программ.

Анализируя приведенные особенности потенциальных угроз безопасности информации в РКС, можно сделать вывод, что все они связаны с передачей информации по каналам связи, с территориальной разобщенностью объектов системы. Таким образом, в РКС наряду с мерами, предпринимаемыми для обеспечения безопасности информации в сосредоточенных КС, реализуется ряд механизмов для защиты информации при передаче ее по каналам связи, а также для защиты от несанкционированного воздействия на информацию КС с использованием каналов связи.

Все методы и средства, обеспечивающие безопасность информации в защищенной вычислительной сети, могут быть распределены по группам:

- обеспечение безопасности информации в пользовательской подсистеме и специализированных коммуникационных КС;
- защита информации на уровне подсистемы управления сетью;
- защита информации в каналах связи;
- обеспечение контроля подлинности взаимодействующих процессов.

Практическая часть

Расширьте модель используемого Вами конкретного предприятия¹, доработав игровую ситуацию следующим образом.

Предприятие включает в себя центральный офис, расположенный в г. Ставрополе и три местных офиса в городах: Невинномысск, Кисловодск и Пятигорск. Все офисы оборудованы ПЭВМ (пять в центральном и по одному в местных) и включены в КС, осуществляющую связь через Internet.

Задание

¹ Предприятие должно было быть Вами выбрано и описано в предыдущем семестре. Дополнительно необходимо предоставить описание этого предприятия. Описание предприятия должно содержать следующие разделы: общее описание (где находится, чем занимается, сколько человек работает, организационная структура, структура производственных процессов), план территории, расположения помещений/помещения предприятия с указанием наименований соответствующих

1. Разработать структурную схему распределенной КС предприятия. При разработке структурной схемы укажите, какие средства коммутации и обеспечения безопасности (программные, аппаратные, наименование, марка, стоимость) используются для объединения компьютеров в офисах и для организации выхода пользователей в интернет.

2. На основе анализа КС предложить методы и средства, обеспечивающие безопасность информации в ней.

Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

Интернет-ресурсы: 1-3

Программное обеспечение: 1-2

подразделений, на плане также должны быть указаны основные конструктивные элементы помещений, расположение источников информации, средств ее обработки, линий связи, коммуникации и пр.

Тема 8. Общая характеристика подходов к оценке эффективности комплексной системы защиты информации

Лабораторная работа 15

Название работы: Системный анализ информационной безопасности и принятие решения по инженерно-технической защите охраняемого объекта

Время 4,5 часа

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Теоретическая часть

Так как не существует формальных методов синтеза вариантов предотвращения угроз безопасности информации, то разработка мер по защите информации проводится эвристическим путем на основе знаний и опыта соответствующих специалистов. Однако в интересах минимизации ошибок процесс разработки должен соответствовать следующим рекомендациям.

Разработку мер защиты информации целесообразно начинать с угроз, имеющих максимальное значение, далее - с меньшей угрозой и так далее до тех пор, пока не будут исчерпаны выделенные ресурсы. Такой подход гарантирует, что даже при малых ресурсах хватит средств для предотвращения наиболее значимых угроз. Для каждой угрозы разрабатываются меры (способы и средства) по защите информации. Перечень типовых способов и средств приведены в таблице 15.1.

Таблица 15.1 - Перечень типовых способов и средств

Способы реализации угроз	Типовые способы и средства предотвращения угроз
Физический контакт злоумышленника с источником информации	Механические преграды (заборы, КПП, двери, взломостойкие стекла, решетки на окнах, хранилища, сейфы), технические средства охраны, телевизионные средства наблюдения, дежурное и охранное освещение, силы и средства нейтрализации угроз.
Воздействие огня	Технические средства пожарной сигнализации, средства пожаротушения - огнестойкие хранилища и сейфы.
Наблюдение	Маскировочное окрашивание, естественные и искусственные маски, ложные объекты, аэрозоли, пены, радиолокационные отражатели, радио- и звукопоглощающие покрытия, тепло-изолирующие материалы, генераторы радио- и гидроакустических помех.

Подслушивание	Скремблирование и цифровое шифрование, звукоизолирующие конструкции, звукоизолирующие материалы, акустическое и вибрационное зашумление, обнаружение, изъятие и разрушение закладных устройств.
Способы реализации угроз	Типовые способы и средства предотвращения угроз
Перехват	Выполнение требований по регламенту и дисциплине связи, отключение источников опасных сигналов, фильтрация и ограничение опасных сигналов, применение буферных устройств, экранирование, пространственное и линейное зашумление.
Утечка информации по материальновещественному каналу	Учет и контролируемое уничтожение черновиков, макетов, брака, сбор и очистка от демаскирующих веществ отходов.

Так как меры по защите информации рассматриваются для каждой угрозы, то в контролируемой зоне возможно их дублирование. Например, полуоткрытая дверь в служебное помещение может способствовать как наблюдению документов и экранов ПЭВМ в помещении, так и подслушиванию ведущихся в нем разговоров. Установленные на дверь устройства для автоматического ее закрытия и кодовый замок предотвращают утечку информации по этим каналам.

Следовательно, разработка мер по предотвращению угроз представляет собой итерационный процесс, каждая итерация которого выполняется в 2 этапа:

- разработка локальных мер по предотвращению каждой из выявленных угроз;
- интеграция (объединение) локальных мер. Условием для перехода к следующей итерации является освобождение в результате объединения способов и средств защиты информации части ресурса. достаточно и "для предотвращения очередной угрозы.

Рекомендуемые способы и средства защиты информации заносятся в таблицу, вариант которой приведен в таблице 15.2.

Таблица 15.2 - Рекомендуемые способы и средства защиты информации

№	Тип угрозы	Величина угрозы (доля от 1)	Способы предотвращения угроз	Средства предотвращения угроз	Затраты на предотвращения угроз
---	------------	-----------------------------	------------------------------	-------------------------------	---------------------------------

1	2	3	4	5	6
Суммарные затраты на защиту информации					

Практическая часть

В качестве объекта анализа используйте организацию, рассмотренную в предшествующих работах. Задание:

1. Проанализировать угрозы, начиная с угроз, имеющих максимальное значение, далее - с меньшей угрозой и так далее до тех пор, пока не будут исчерпаны выделенные ресурсы.
2. Принять решение по инженерно-технической защите охраняемого объекта, результаты оформить таблицей 2.

Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

Интернет-ресурсы: 1-3

Программное обеспечение: 1-2

Лабораторная работа 16

Название работы: Системный анализ информационной безопасности и принятие решения по ее защите с использованием комплексной системы защиты информации

Время 4,5 часа

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Цель работы:

- изучить теоретический материал;
- получить практические навыки и умения по организации комплексной защиты объекта.

Теоретическая часть

Система контроля и управления доступом "ПРОХОДНАЯ-М" с одной точкой прохода через турникет и организацией контроля доступа для четырех точек прохода внутри предприятия.

Предлагаемая система для контроля и управления доступом выполнена на базе программного комплекса TSS-2000Profi.

Система предназначена для решения задачи автоматизированного контроля и управления входом/выходом на территорию предприятия персонала и посетителей через проходную, а также для контроля доступа во внутренние помещения предприятия (в данном случае - четыре комнаты).

Система также позволяет организовать учет рабочего времени сотрудников, получать разнообразные отчеты о событиях в системе.

Система может быть использована на небольших предприятиях и организациях.

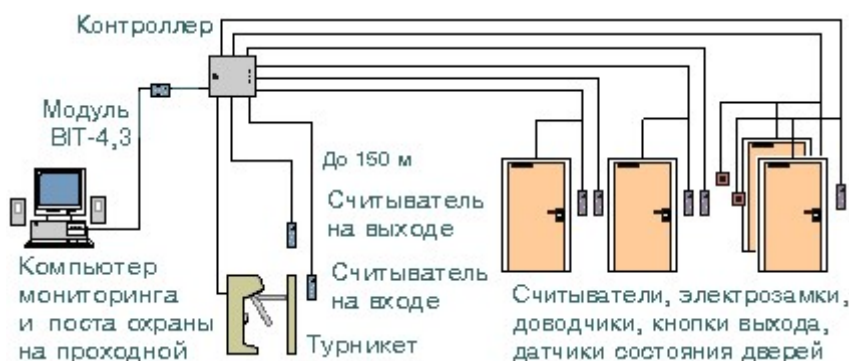


Рисунок 16.1 - Структурная схема СКУД «ПРОХОДНАЯ-М»

Окно регистрации владельцев "электронных ключей" и задания для них ограничений доступа. Каждый сотрудник или посетитель предприятия получает идентификатор ("электронный ключ") - пластиковую карточку или брелок с содержащимся в ней индивидуальным кодом. "Электронные

ключи" выдаются в результате регистрации перечисленных лиц с помощью средств системы. Паспортные данные и другие сведения о доступе владельца "электронного ключа" заносятся в персональную "электронную карточку". Персональная "электронная карточка" владельца и код его "электронного ключа" связываются друг с другом и заносятся в специально организованные компьютерные базы данных. Имеется возможность поиска, сортировки и отбора в базе данных "электронных карточек" зарегистрированных владельцев ключей по самым различным критериям.

Затем происходит загрузка кодов "электронных ключей" в контроллер и программирование контроллера с помощью программного обеспечения. Вы имеете возможность на основе алгоритмов программного обеспечения:

- ☐ легко и наглядно загружать и выборочно удалять из памяти контроллера коды "электронных ключей", предназначенных для прохода,
- ☐ задавать объектовые и временные ограничения доступа как для отдельных владельцев ключей, так и для групп владельцев, выделенных по какому-либо признаку,
- ☐ для каждого из зарегистрированных в системе ключей можно определить срок его действия,
- ☐ при установке ограничений доступа для владельца ключа можно задать номера зон доступа, представляющих собой списки дверей, через которые данный владелец может входить и выходить из помещений и здания.

У входа на предприятие (в проходной) на панели турникета или рядом с ним устанавливается считыватель, считывающий с карточек их код и передающий эту информацию в контроллер системы.

Работник организации или посетитель, имеющий "электронный ключ", подходит к турникету и предъявляет его считывателю.

Одновременно с этим на экране компьютера, установленного на проходной, появляется изображение и основная информация о владельце "ключа", занесенная в базу данных системы.

В системе каждому коду поставлена в соответствие информация о правах доступа владельца карточки. На основе сопоставления этой информации и ситуации, при которой была предъявлена карточка, система

принимает решение: контроллер открывает или блокирует проход через турникет.

Если в данное время для владельца предъявленного "электронного ключа", разрешен проход через турникет, система автоматически разблокирует его. Если же действует запрет на проход или предъявлен незарегистрированный "ключ", то турникет останется в заблокированном состоянии, а на экране компьютера поста охраны появится надпись о запрете с указанием причины отказа в доступе. Одновременно с этим компьютер воспроизводит соответствующее речевое сообщение. Например: "Вход заблокирован. Истек срок действия ключа!" или "Запрет по времени!", "Внимание! Предъявлен неизвестный ключ!" и т.п.

Сотрудник службы безопасности, дежурящий на проходной, в любой момент времени может вмешаться в работу системы - сравнить фотографию на экране и входящего человека, а затем заблокировать или разблокировать турникет, нажав кнопку клавиатуры компьютера или выносного пульта управления турникетом.

Подобным же образом регулируется и выход с предприятия. Причем, в том случае, если выходящий человек является посетителем Вашей организации, получившим разовый пропуск (ключ), система напомнит дежурному на проходной о необходимости изъятия у него временно выданного ключа звуковым или речевым сообщением типа: "Внимание, гость! Просьба забрать ключ".

Контроль доступа во внутренние помещения. В системе также осуществляется контроль доступа во внутренние помещения предприятия (в предлагаемой системе - четыре комнаты). Причем в особо важных помещениях (например, бухгалтерия, склад или др.) считыватели устанавливаются на входе и выходе, а в других комнатах - только на входе. Выход из этих помещений осуществляется при нажатии на кнопку выхода.

На основе сопоставления информации о правах доступа и ситуации, при которой был предъявлен "ключ", система принимает решение: контроллер открывает или блокирует проход через двери, переводит помещение в режим охраны, включает сигнал тревоги и т.д.

Все факты предъявления "ключей" и связанные с ними действия (проходы, факты срабатывания датчика и нажатия кнопки турникета и т.д.) фиксируются в контроллере, автоматически заносятся в журналы событий,

связанные с проходом через турникет проходной и двери внутренних контролируемых помещений. Причем, для каждого события указывается: его характер, дата, время, код предъявляемого "ключа" и Ф.И.О. его владельца или дежурного оператора, нажавшего кнопку. Информацию об этих событиях в любой момент можно просмотреть на экране компьютера.

Получение отчетов

Программное обеспечение системы позволяет вести учет рабочего времени сотрудников и посетителей, которым выданы "ключи", получать разнообразные отчеты о событиях в системе за выбранные промежутки времени. Например:

- ☐ все события (информация о всех или произвольно выбранных событиях);
- ☐ нарушения (информация о нарушениях рабочего графика);
- ☐ проходы (информация о проходах в помещения всех или выбранных лиц;
- ☐ рабочее время (учет рабочего времени всех или выбранных лиц).

Момент первого входа через проходную, интерпретируется системой в процессе учета рабочего времени как начало, а момент последнего выхода - как конец рабочего дня владельца предъявленного электронного ключа.

Если в течение рабочего дня какому-либо сотруднику необходимо неоднократно входить и выходить через проходную, то при формировании отчетов о рабочем времени, система суммирует отдельные промежутки времени пребывания его на территории организации.

Важной особенностью системы является то, что любой владелец ключа, проникший в здание, минуя проходную (код его ключа не был считан считывателем на входе проходной), не сможет войти ни в одну из контролируемых системой дверей.

Следует отметить, что в число речевых сообщений о событиях помимо стандартных могут также входить и произвольные сообщения, связанные с доступом в каждое из помещений и самостоятельно записанные администратором системы с помощью микрофона.

Содержание и величина сообщения не регламентируются, - это позволяет гибко учитывать особенности контролируемых объектов,

дополнять список и изменять содержание экстренных сообщений при изменении состава или переустановке оборудования системы.

При необходимости проводить визуальный мониторинг объектов можно также и в режиме отображения поэтажных планов, на которых наглядно отображается ситуация в здании.

Контролируемые пункты прохода в помещения обозначаются на планах пиктограммами или значками, вид или цвет которых может меняться в зависимости от состояния соответствующего объекта. (Например, в случае блокировки оператором какой-либо двери, ее пиктограмма на поэтажном плане приобретает желтую подсветку, а при взломе двери периодически вспыхивает красным цветом).

В момент возникновения нештатного события на экране компьютера автоматически или по команде пользователя разворачивается план нужного этажа, на котором указывается место или объект, с которым связано тревожное событие. Это позволяет даже наиболее слабо подготовленному оператору быстро оценить ситуацию, подтвердить получение сигнала тревоги и принять правильное решение.

После принятия решения оператор системы с помощью клавиатуры компьютера, мыши или выносного пульта управления исполнительным устройством может дистанционно открыть или заблокировать какую-либо отдельную дверь, открыть все двери в случае пожара или заблокировать их в момент нападения, активизировать системы пожаротушения, включить сирену и т.д.

Система может круглосуточно функционировать в двух основных режимах: в комплексном, при котором работой системы управляет компьютер мониторинга, и в автономном режиме работы контроллера.

В автономный режим система переходит:

○ по команде администратора системы (например, в случае необходимости замены или подключения какого-либо элемента, перед проведением профилактики и т.д.)

○ автоматически через три секунды после пропадания связи между контроллером и компьютером в результате повреждения линии связи, отключении электричества в здании, при выходе из строя компьютера.

В этом режиме контроллер управляет проходом через проходную и доступом в помещения владельцев тех "электронных ключей", коды

которых были занесены в память контроллера, а также фиксирует в памяти информацию о событиях, связанных с проходами через эти точки прохода. После запуска программного обеспечения и перехода системы в сетевой режим эта информация автоматически переписывается в "системный журнал" компьютера.

Регулирование доступа осуществляется только с учетом полных запретов на доступ в то или иное помещение, а временные интервалы запрета доступа не учитываются. Работает только режим контроля прохода через турникет, а режимы показа фотографий не работают.

Продолжительность автономной работы системы в случае отсутствия электропитания в сети может достигать 8 часов.

Доступ к базе "электронных карточек", содержащих информацию о зарегистрированных владельцах ключей, открыт только для уполномоченных сотрудников после ввода личного кода.

Контроллеры TSS-201-8W/8T В

памяти контроллера сохраняется:

- ☐ 2000 кода
- ☐ 2000 сообщения о событиях

Контроллеры серии TSS-201-8W, TSS-201-8T имеют восемь портов, к каждому из которых можно подключить оборудование одной точки прохода.

Каждый из портов контроллера включает в себя:

- ☐ канал для подключения считывателя;
- ☐ канал для подключения датчика состояния пункта прохода (двери);
- ☐ канал для подключения кнопки открывания двери;
- ☐ релейный выход для управления исполнительным устройством.

Контроллер имеет энергонезависимую память, встроенный календарь-часы.

Интерфейс подключаемых считывателей: Т - для считывателей идентификаторов типа Touch Memory, W- для считывателей с интерфейсом Wiegand (26-48 бит).

Элементы оборудования пунктов прохода через проходную:

☐ считыватели на вход и на выход (считывают код карточки-ключа пользователя и обеспечивают его ввод в контроллер при проходе через турникет);

☐ турникет;

☐ пульт (кнопка) управления турникетом.

Элементы оборудования пункта прохода через дверь:

☐ считыватели на вход и на выход (считывают код карточки-ключа пользователя и обеспечивают его ввод в контроллер при проходе через дверь);

☐ датчик состояния двери (служит для сигнализации о взломе двери, а если дверь слишком долго находится в открытом положении, система

сообщает об этом и заносит этот факт в "системный журнал");

☐ электрозамок;

☐ доводчик двери.

Компьютер

Компьютер проходной является компьютером мониторинга системы и непосредственно компьютером проходной. Компьютер выводит данные из электронной базы непосредственно охраннику на пункт прохода при прохождении через турникет владельца пропуска, а также разнообразные отчеты о событиях в системе за выбранные промежутки времени.

В составе системы используются обычные IBM-совместимые компьютеры со следующими параметрами:

☐ процессором типа Pentium, Celeron,

☐ оперативной памятью объемом не менее 64 Мб,

☐ SVGA-монитором и видеокартой, поддерживающими разрешение не менее 800х600 точек и глубину цвета в 24 бита (16,7млн. цветов).

Практические вопросы 4.

Проанализировать пример.

5. Составить перечень приборов из которых должна состоять система если используется Вариант с Proximity считывателями (рисунки 16.2, 16.3).

6. Рассчитать примерную стоимость оборудования по прайсам в Internet.

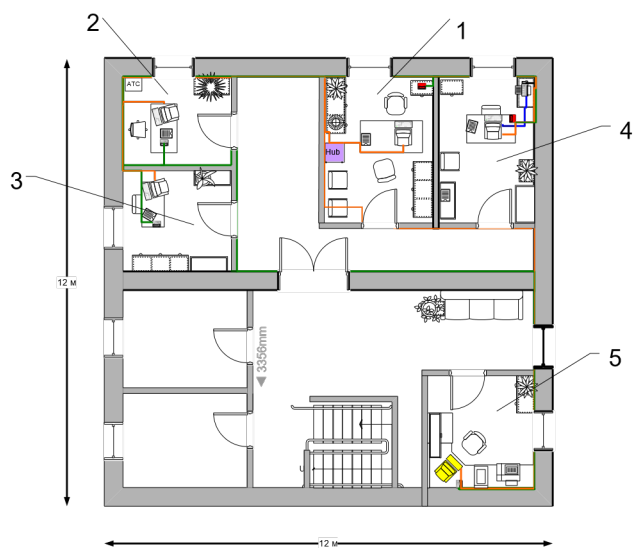
Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

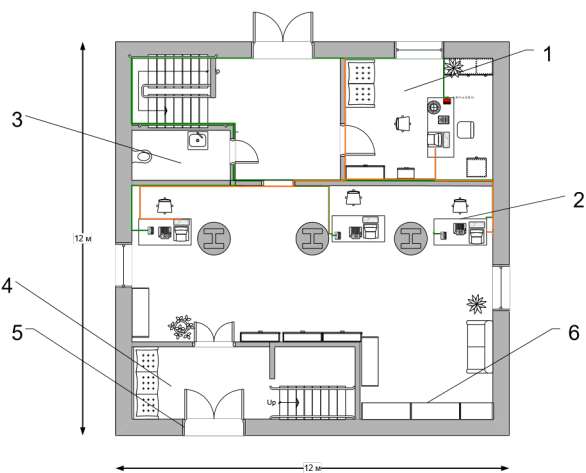
Интернет-ресурсы: 1-3

Программное обеспечение: 1-2



- 1 - Кабинет директора
- 2 - Кабинет заместителя директора
- 3 - Кабинет главного бухгалтера
- 4 - Кабинет секретаря
- 5 - Кабинет программиста
- - телефон с общегородским номером
- - телефон для внутренней связи
- - подключение АРМ к НАВ

ATC
 ■ - факс - модем
 ■ - сервер



- 1 - Офис менеджера
- 2 - Рабочие места продавцов-кассиров в торговом зале
- 3 - Подсобное помещение (туалет)

■
 ■
 — - подключение телефонов к АТС организации
 4 - Холл

- 5 - Центральный вход в здание
- 6 - Выставка продукции

- подключение телефонов к АТС организации
- телефон с общегородским номером
- АТС организации
- телефон для внутренней связи
- подключение АРМ к НАВ

Рисунок 16.2 – Схема этажа

ПРИЛОЖЕНИЕ А (обязательное)

Перечень защищаемой информации

- ☐ сведения о решениях руководства по коммерческим вопросам;
- ☐ сведения, содержащихся в документах, дающих право на осуществление предпринимательской деятельности;
- ☐ планы инвестиций предприятия;
- ☐ списки клиентуры;
- ☐ карточки клиентов;
- ☐ сведения, содержащиеся в бухгалтерских книгах предприятия;
- ☐ сведения о плановых и фактических показателях финансового плана;
- ☐ уровень доходов предприятия;
- ☐ о системе оплаты труда;
- ☐ планово-аналитические материалы за текущий период;
- ☐ о состоянии противопожарной безопасности;
- ☐ сведения о перспективных методах управления производством;
- ☐ планы развития предприятия;
- ☐ сведения о поставщиках;
- ☐ состояние рынка сбыта и перспектив рыночной конъюнктуры;
- ☐ обзоры рынка;
- ☐ рыночная стратегия предприятий;
- ☐ сведения об эффективности коммерческой деятельности предприятия;
- ☐ о наличии свободных рабочих мест;
- ☐ сведения о планах предприятия по расширению производства;
- ☐ стоимость товарных запасов;
- ☐ о социальным выплатам;

- ☐ банковские операции;
 - ☐ источники кредитов и условия по ним;
 - ☐ план производства и перспективный план;
 - ☐ результаты маркетинговых исследований;
 - ☐ коммерческие связи;
 - ☐ о нарушениях законодательства Российской Федерации;
 - ☐ сведения о потребителях;
 - ☐ о задолженности по выплате заработной платы ☐
- сведения о продажах товара на новых рынках;
- ☐ об условиях труда.

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

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению практических работ

по дисциплине «Комплексная система защиты информации на предприятии»

для студентов направления подготовки

10.03.01 «Информационная безопасность» Направленность (профиль)

«Организация и технологии защиты информации (по отрасли или в сфере
профессиональной деятельности)»

Ставрополь

2026

115

СОДЕРЖАНИЕ

Практическое занятие 1 Сущность и общее содержание комплексной системы защиты информации	
Практическое занятие 2 Принципы организации и требования, предъявляемые к комплексной системе защиты информации	
Практическое занятие 3 Определение и нормативное закрепление состава защищаемой информации	
Практическое занятие 4 Определение состава компонентов и условий функционирования комплексной системы защиты информации	
Практическое занятие 5 Разработка модели, технологическое и организационное построение комплексной системы защиты информации ...	
Практическое занятие 6 Моделирование способов физического проникновения злоумышленника к источникам информации	
Практическое занятие 7 Моделирование угроз безопасности информации	
Практическое занятие 8 Разработка организационных и технических мер по инженерно-технической защите информации	
Практическое занятие 9 Система контроля и управления доступом	

ВВЕДЕНИЕ

■ 1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины является формирование профессиональных компетенций в области комплексной системы защиты информации, методики и технологии ее организации на предприятии, принципов и содержания управления системой, методов обеспечения ее надежности.

Задачи освоения дисциплины...

- дать основы сущности, целей и задач комплексной системы защиты информации, принципов и этапов ее разработки;
- освоить технологии установления состава защищаемой информации и объектов защиты, получить необходимые знания по методам оценки уязвимости защищаемой информации;
- научиться определять параметры и структуру комплексной системы защиты информации, проведению мероприятий по обеспечению функционирования комплексной системы защиты информации;
- познакомить со структурой и методами управления комплексной системой защиты информации, подходами к определению показателей эффективности и методиками ее оценки.

■ 2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
-------------------------------	------------------------------	---

ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ИД-1 Использует методологический базис теории защиты информации, используемый при разработке формировании политики информационной безопасности ИД-2 Осуществляет организацию и поддерживает выполнение комплекса мер по обеспечению информационной безопасности на объекте защиты в качестве технического специалиста ИД-3 Управляет процессом выполнения комплекса мер по обеспечению информационной безопасности реализации на объекте защиты в качестве технического специалиста	ИД-1 Уверенно использует методологический базис теории защиты информации, используемый при разработке формировании политики информационной безопасности ИД-2 Уверенно осуществляет организацию и поддерживает выполнение комплекса мер по обеспечению информационной безопасности на объекте защиты в качестве технического специалиста ИД-3 Способен управлять процессом выполнения комплекса мер по обеспечению информационной безопасности реализации на объекте защиты в качестве технического специалиста
ОПК-2.2 Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы	ИД-1 Демонстрирует понимание оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих, а также устойчивости к деструктивным воздействиям на информационные ресурсы предприятия	ИД-1 Уверенно демонстрирует понимание оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих, а также устойчивости к деструктивным воздействиям на

		информационные ресурсы предприятия
	ИД-2 Демонстрирует способность формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих	ИД-2 Уверенно демонстрирует способность формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих
	ИД-3 Показывает понимание сущности управления проектами по защите информации по заданной методике и экономику защиты информации	ИД-3 Показывает рациональное понимание сущности управления проектами по защите информации по заданной методике и экономику защиты информации
	ИД-4 Демонстрирует способность к реализации проведения экспериментов по заданной методике и обработку их результатов	ИД-4 Уверенно демонстрирует способность к реализации проведения экспериментов по заданной методике и обработку их результатов

ОПК-2.3 Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	ИД-1 Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности защите персональных данных в информационных системах ИД-2 Способен разрабатывать, внедрять и сопровождать комплекс мер по управлению проектами по защите информации по заданной методике и экономику защиты информации ИД-3 Демонстрирует знания комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов	ИД-1 Демонстрирует способность разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности защите персональных данных в информационных системах ИД-2 Разрабатывает, внедряет и сопровождает комплекс мер по управлению проектами по защите информации по заданной методике и экономику защиты информации ИД-3 Уверенно демонстрирует знания комплекса мер по обеспечению безопасности объекта защиты с применением
	информационной безопасности ИД-4 Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	локальных нормативных актов и стандартов информационной безопасности ИД-4 Демонстрирует способность разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности

ОПК-2.4 Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами	ИД-1 Организует по аудиту защищенности объекта информатизации в соответствии с нормативными документами	ИД-1 Уверенно организует мероприятия по аудиту защищенности объекта информатизации в соответствии с нормативными документами
	ИД-2 Проводит защищенности информатизации в соответствии с нормативными документами	ИД-2 Умеет проводить аудит защищенности объекта информатизации в соответствии с нормативными документами
	ИД-3 Демонстрирует процедур защищенности информатизации нормативных документов, определяющих содержание	ИД-3 Демонстрирует уверенные знания процедур аудита защищенности объекта информатизации и нормативных документов, определяющих его содержание
	ИД-4 Осуществляет защищенности информатизации в соответствии с нормативными документами	ИД-4 Способен осуществлять аудит защищенности объекта информатизации в соответствии с нормативными документами

Практическое занятие 1

Название работы: Сущность и общее содержание комплексной системы защиты информации

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Теоретическая часть

Организация и функционирование комплексной системы безопасности должны осуществляться на основе следующих принципов.

1. Комплексность:

- обеспечение безопасности персонала, материальных и финансовых ресурсов от возможных угроз всеми доступными законными средствами, методами и мероприятиями;

- обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их обработки (преобразования) и использования, во всех режимах функционирования;

- способность системы к развитию и совершенствованию в соответствии с изменениями условий функционирования фирмы;

2. Своевременность – упреждающий характер мер обеспечения безопасности. Своевременность предполагает постановку задач по комплексной безопасности на ранних стадиях разработки системы безопасности на основе анализа и прогнозирования обстановки, угроз безопасности, а также разработку эффективных мер предупреждения посягательств на законные интересы.

3. Непрерывность – считается, что злоумышленники только и ищут возможность, как бы обойти защитные меры, прибегая для этого к легальным и нелегальным методам.

4. Активность. Защищать интересы фирмы необходимо с достаточной степенью настойчивости, широко используя маневр силами и средствами обеспечения безопасности и нестандартные меры защиты.

5. Законность. Предполагает разработку системы безопасности на основе федерального законодательства в области предпринимательской деятельности, информатизации и защиты информации, частной охранной деятельности, а также других нормативных актов по безопасности, утвержденных органами государственного управления в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений.

6. Обоснованность. Предлагаемые меры и средства защиты должны реализоваться на современном уровне развития науки и техники, быть обоснованными с точки зрения заданного уровня безопасности и соответствовать установленным требованиям и нормам.

7. Экономическая целесообразность и сопоставимость возможного ущерба и затрат на обеспечение безопасности (критерий "эффективность – стоимость").

8. Специализация. Предполагается привлечение к разработке и внедрению мер и средств защиты специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Эксплуатация технических средств и реализация мер безопасности должны осуществляться профессионально подготовленными специалистами службы безопасности, ее функциональных и обслуживающих подразделений.

9. Взаимодействие и координация. Предполагает осуществление мер обеспечения безопасности на основе четкого взаимодействия всех заинтересованных подразделений и служб, сторонних специализированных организаций в этой области, координацию их усилий для достижения поставленных целей, а также интеграцию деятельности с органами государственного управления и правоохранительными органами.

10. Совершенствование. Предусматривает совершенствование мер и средств защиты на основе собственного опыта, появления новых технических средств с учетом изменений в методах и средствах разведки и промышленного шпионажа, нормативно-технических требований, накопленного отечественного и зарубежного опыта.

11. Централизация управления. Предполагает самостоятельное функционирование системы безопасности по единым организационным, функциональным и методологическим принципам с централизованным управлением деятельностью системы безопасности.

Особое внимание необходимо уделять принципу комплексности. Для обеспечения безопасности во всем многообразии структурных элементов фирмы, при множестве угроз и способов несанкционированного доступа должны применяться все виды и формы защиты и противодействия в полном объеме. Недопустимо применять отдельные формы или технические средства.

Комплексный подход предполагает учет в управлении объектом всех основных его аспектов, и все элементы управляемой системы рассматриваются только в совокупности, целостности, единстве. Таким образом, необходимо создание комплексной системы защиты информации на предприятии.

Комплексная система защиты информации на предприятии – это совокупность взаимосвязанных мероприятий организационно-правового характера, осуществляемых в целях защиты предприятия от реальных или потенциальных действий физических или юридических лиц, которые могут привести к существенным потерям.

Основной целью системы безопасности предприятия является предотвращение ущерба ее деятельности за счет разглашения, утечки и несанкционированного доступа к источникам конфиденциальной информации; хищения финансовых и материально-технических средств; уничтожения имущества и ценностей; нарушения работы технических средств обеспечения производственной деятельности, включая и средства информатизации, а также предотвращение ущерба персоналу фирмы.

Целями комплексной системы защиты информации являются:

1. Защита прав предприятия, его структурных подразделений и сотрудников;
2. Сохранение и эффективное использование финансовых, материальных и информационных ресурсов;
3. Повышение имиджа и роста прибылей за счет обеспечения качества услуг и безопасности клиентов.

Задачами комплексной системы защиты информации являются:

1. Своевременное выявление и устранение угроз персоналу и ресурсам; причин и условий, способствующих нанесению финансового, материального и морального ущерба интересам фирмы, нарушению ее нормального функционирования и развития;
2. Отнесение информации к категории ограниченного доступа (служебной и коммерческой тайнам, иной конфиденциальной информации, подлежащей защите от неправомерного использования) и других ресурсов – к различным уровням уязвимости (опасности) и подлежащих сохранению;
3. Создание механизма и условий оперативного реагирования на угрозы безопасности и проявления негативных тенденций в функционировании фирмы;
4. Эффективное пресечение посягательств на ресурсы и угроз персоналу на основе комплексного подхода к безопасности;
5. Создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями физических

и юридических лиц, для ослабления негативного влияния последствий нарушения безопасности на достижение стратегических целей.

Практическая часть

Задания (необходимо ответить письменно).

1. Выделите основные свойства систем (не менее 5).
2. Сформулируйте свой вариант определения понятия «комплексная система защиты информации».
3. Сформулируйте свой вариант определения понятия «цель организации и функционирования комплексной системы защиты информации»
4. Разработайте пирамиду целей комплексной системы защиты информации (результат представьте в виде схемы, или таблицы)
5. Определите основные классы задач комплексной системы защиты информации и дайте их краткую и обобщенную характеристику (не менее 4 классов, результат представьте в виде таблицы)

Таблица 1.1 – Основные классы задач комплексной системы защиты информации и их характеристика

Класс задач

п.п.	комплексной системы защиты класса задач	Краткая	Обобщенная №
		характеристика	характеристика информации
		класса	

Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

Интернет-ресурсы: 1-3

Программное обеспечение: 1-2

Практическое занятие 2

Название работы: Принципы организации и требования, предъявляемые к комплексной системе защиты информации

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Теоретическая часть

Основные принципы организации комплексных систем защиты информации во многом совпадают с принципами организации сложных человеко-машинных систем, но существуют и некоторые специфические принципы. Кроме того, различна содержательная интерпретация принципов в зависимости от вида и назначения системы.

Прежде, чем приступать к разработке системы информационной безопасности, необходимо определить, что же для организации (физического лица) является интеллектуальной собственностью.

С точки зрения делового человека, *интеллектуальной собственностью являются информационные ресурсы, знания, которые помогают ему эффективно разрабатывать и изготавливать новую продукцию, выгодно продавать товар или каким-то другим образом увеличивать свою прибыль.* Способ управления производством, технологический процесс, список клиентов, профиль научных исследований, анализ конкурентоспособности – лишь некоторые примеры тому.

Незнание того, что составляет интеллектуальную собственность – уже шаг к потерям финансовым, моральным и материальным. Именно с этого надо начинать создание системы защиты информации.

Дальнейшими этапами, вне зависимости от размеров организации и специфики ее информационной системы, в том или ином виде должны быть:

- ☐ определение границ управления информационной безопасностью объекта;
- ☐ анализ уязвимости;
- ☐ выбор контрмер, обеспечивающих информационную безопасность; определение политики информационной безопасности;
- ☐ проверка системы защиты;
- ☐ составление плана защиты;
- ☐ реализация плана защиты (управление системой защиты).

Любые действия по созданию системы информационной безопасности должны заканчиваться определенными результатами в виде документа или технического решения.

средств и мероприятий) обеспечения безопасности информации не является надежным, а максимальный эффект достигается при объединении всех их в целостную систему защиты информации. Только оптимальное сочетание организационных, технических и программных мероприятий, а также постоянное внимание и контроль над поддержанием системы защиты в актуальном состоянии позволит с наибольшей эффективностью обеспечить решение постоянной задачи.

Как показывает разработка реальных систем, ни один из способов (мер средств и мероприятий) обеспечения безопасности информации не является надежным, а максимальный эффект достигается при объединении всех их в целостную систему защиты информации. Только оптимальное сочетание организационных, технических и программных мероприятий, а также постоянное внимание и контроль над поддержанием системы защиты в актуальном состоянии позволит с наибольшей эффективностью обеспечить решение постоянной задачи.

Методологические основы обеспечения информационной безопасности являются достаточно общими рекомендациями, базирующимися на мировом опыте создания подобных систем. Задача каждого специалиста по защите информации преломить абстрактные положения к своей конкретной предметной области (предприятию, организации, банка), в которых всегда найдутся свои особенности и тонкости этого не простого ремесла.

Практическая часть

Задания (необходимо ответить письменно).

1. Раскройте сущность следующих принципов организации сложных организационно-технических систем: целенаправленность, комплексность, научная обоснованность, экономичность, эргономичность, централизованность, специализированность, совершенствование (результат представьте в виде таблицы)

Таблица 2.1 – Принципы организации сложных организационнотехнических систем

№ п.п.	Наименование принципа	Сущность принципа

2. Из перечня принципов пункта 1 укажите принципы организации сложных социотехнических систем, обоснуйте свой выбор (результат представьте в виде таблицы).

Таблица 2.2 – Принципы организации сложных социотехнических систем

№ п.п.	Наименование принципа	Обоснование

3. Укажите, какими принципами следует руководствоваться при организации и управлении комплексной системой защиты информации. Укажите приоритетность выбранных принципов, используя практические примеры (результат представьте в виде таблицы).

Таблица 2.3 – Принципы организации и управления комплексной системой защиты информации

№ п.п.	Наименование принципа	Приоритет

Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

Интернет-ресурсы: 1-3

Программное обеспечение: 1-2

Практическое занятие 3

Название работы: Определение и нормативное закрепление состава защищаемой информации

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Теоретическая часть

Информацию относят к защищаемой в зависимости от того:

- ☐ сколько за нее заплачено;
- ☐ сколько потеряют в случае ее потери или разглашения;

Критерии отнесения к различным грифам:

- ☐ количественная оценка стоимости информации;
- ☐ длительность жизненного цикла;
- ☐ возможности предприятия (фин., техн., экон.); ☐ вид деятельности.

Требования обеспечения безопасности и защиты информации фирмы отражаются в уставе (учредительном договоре) в виде следующих положений:

- ☐ предприятие имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, требовать от своих сотрудников обеспечения их сохранности и защиты от внутренних и внешних угроз;
- ☐ предприятие обязано обеспечить сохранность конфиденциальной информации.

Такие требования дают право администрации предприятия:

- ☐ создавать организационные структуры по защите конфиденциальной информации;
- ☐ издавать нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;
- ☐ включать требования по защите информации в договоры по всем видам хозяйственной деятельности;

○ требовать защиты интересов предприятия со стороны государственных и судебных инстанций;

○ распоряжаться информацией, являющейся собственностью предприятия, с целью извлечения выгоды и недопущения экономического ущерба коллективу предприятия и собственнику средств производства;

○ разработать «Перечень сведений конфиденциальной информации».

Требования правовой обеспеченности защиты информации предусматриваются в коллективном договоре, который должен содержать следующие требования:

В разделе «Предмет договора».

Администрация предприятия (в том числе и администрация самостоятельных подразделений) ОБЯЗУЕТСЯ обеспечить разработку и осуществление мероприятий по определению и защите конфиденциальной информации.

Трудовой коллектив принимает на себя обязательства по соблюдению установленных на предприятии требований по защите конфиденциальной информации.

Администрация обязана учесть требования защиты конфиденциальной информации в правилах внутреннего распорядка.

В разделе «Кадры. Обеспечение дисциплины труда».

Администрация обязуется: нарушителей требований по защите коммерческой тайны привлекать к административной и уголовной ответственности в соответствии с действующим законодательством.

В разделе «Порядок приема и увольнения рабочих и служащих».

○ при поступлении рабочего или служащего на работу или переводе его в установленном порядке на другую работу, связанную с конфиденциальной информацией предприятия, а также при увольнении администрация обязана проинструктировать работника или служащего по правилам сохранения коммерческой тайны с оформлением письменного обязательства о ее неразглашении;

☐ администрация предприятия вправе принимать решение об отстранении от работ лиц, которые нарушают установленные требования по защите конфиденциальной информации.

В разделе «Основные обязанности рабочих и служащих».

Рабочие и служащие обязаны соблюдать требования нормативных документов по защите конфиденциальной информации предприятия.

В разделе «Основные обязанности администрации».

Администрация предприятия, руководители подразделений обязаны:

☐ обеспечить строгое сохранение конфиденциальной информации, постоянно осуществлять организаторскую и воспитательно-профилактическую работу, направленную на защиту секретов предприятия;

☐ включить в должностные инструкции и положения обязанности по сохранению конфиденциальной информации;

☐ неуклонно выполнять требования устава, коллективного договора, трудовых договоров, правил внутреннего трудового распорядка и других организационных и хозяйственных документов по обеспечению экономической и информационной безопасности.

Обязательства конкретного сотрудника, рабочего или служащего по защите информации обязательно должны быть оговорены в трудовом договоре (контракте), при заключении которого трудящийся обязуется выполнять определенные требования, действующие на данном предприятии. Независимо от формы заключения договора (устного или письменного) подпись трудящегося на приказе о приеме на работу подтверждает его согласие с условиями договора.

Практическая часть

Задания (необходимо ответить письменно).

1. Разработайте классификацию видов тайн (результат представьте в виде схемы, или таблицы)

2. Укажите нормативно правовые акты, в которых закрепляется состав защищаемой/открытой информации, приведите выдержки из нормативных актов с указанием конкретных видов информации (результат представьте в виде таблицы)

Таблица 3.1 – Нормативно правовые акты, закрепляющие состав защищаемой/открытой информации

№ п.п.	Наименование нормативно-правового акта	Выдержка из акта

3. Разработайте алгоритм, согласно которому необходимо действовать при определении состава защищаемой информации на предприятии

(результат представьте в виде таблицы).

Таблица 3.2 – Алгоритм при определении состава защищаемой информации

№ п.п.	Описание шага алгоритма

4. Опишите методику составления Перечня сведений, составляющих коммерческую тайну предприятия. Укажите функции должностных лиц, объединений и основных структурных подразделений (в произвольной форме с явным выделением этапов методики).

Таблица 3.3 – Методика составления Перечня сведений, составляющих коммерческую тайну предприятия

№ п.п.	Описание этапа методики

5. Разработайте Перечень сведений, составляющих коммерческую тайну предприятия согласно выбранному номеру варианта. Результаты представьте в виде таблицы.

Таблица 3.4 – Перечень сведений, составляющих коммерческую тайну предприятия

№ п.п.	Категория информации	Подкатегория информации	Вид информации	Носитель информации

При выполнении этого задания рекомендуется использовать результаты выполнения пункта 3 и пункта 4 настоящего занятия. Также рекомендуется предварительно определить категории (разделы) и подкатегории (подразделы) информации, циркулирующей на предприятии. Рекомендуется воспользоваться открытыми источниками информации для анализа деятельности предприятия.

Таблица 3.5 – Перечень предприятий для выполнения практических заданий

Вариант	Наименование предприятия
1	ГОУ ВПО Ставропольский государственный университет
2	ОАО Северо-кавказский банк Сбербанка России, г. Ставрополь
3	ОАО «Ставропольские городские аптеки»
4	ОАО Супермаркет "Тройка", г. Ставрополь
5	МУП "Водоканал", г. Ставрополь
6	МУП "Земельная палата", г. Ставрополь
7	ОАО Концерн "Энергомера"
8	ОАО ПНК "Эском"
9	ОАО "АРНЕСТ"
10	Компания "КАВМИНВОДЫАВИА"

Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

Интернет-ресурсы: 1-3

Программное обеспечение: 1-2

Практическое занятие 4

Название работы: Определение состава компонентов и условий функционирования комплексной системы защиты информации

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Теоретическая часть

Совокупность объектов защиты информации может быть установлена исходя из анализа ряда определений, приведенных в Государственном стандарте Российской Федерации Р 51275 – 99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»

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.

Информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, информационных системах других видов).

Информационная технология – приемы, способы и методы применения технических и программных средств при выполнении функций обработки информации.

Обработка информации – совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения информации.

Система обработки информации – совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала, обеспечивающая выполнение автоматизированной обработки информации.

Средства обеспечения объекта информатизации – технические средства и системы, их коммуникации, не предназначенные для обработки

информации, но устанавливаемые вместе со средствами обработки информации на объекте информатизации.

Система защиты информации – совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Таким образом, к источникам защищаемой информации (объектам защиты) относятся:

- персонал предприятия, а также подчиненных или взаимодействующих предприятий (организаций), допущенный к информации с ограниченным доступом в установленном порядке или могущий ознакомиться с такой информацией, в том числе непреднамеренно;

- материальные средства, содержащие информацию ограниченного доступа (оборудование, материалы, здания, сооружения, хранилища, транспорт и т.д.);

- информационные ресурсы с ограниченным доступом (информация на бумажной, магнитной, оптической основе, информационные массивы и базы данных, программное обеспечение, информативные физические поля различного характера);

- средства и системы информатизации (автоматизированные системы и вычислительные сети различного уровня и назначения, линии, технические средства передачи информации, вспомогательные средства и системы);

- технические средства и системы охраны и защиты материальных и информационных ресурсов.

Средства обеспечения объекта информатизации – технические средства и системы, их коммуникации, не предназначенные для обработки информации, но устанавливаемые вместе со средствами обработки информации на объекте информатизации.

К ним относятся:

- электробытовые приборы (нагревательные, осветительные, вентиляции и т.п.);

- ☐ средства часофикации;
- ☐ системы кондиционирования воздуха;
- ☐ электроосветительные приборы;
- ☐ системы электроснабжения;
- ☐ системы заземления;
- ☐ электронные системы регулирования доступа в помещения;
- ☐ средства видеонаблюдения,
- ☐ системы отопления, водоснабжения, канализации, вентиляции;
- ☐ системы сигнализации и оповещения;
- ☐ системы пожаротушения;
- ☐ средства механизации (бумагоуничтожающие машины, электронные и электрические замки, электрические звонки и т.п.).

Практическая часть

Задания (необходимо ответить письменно).

1. Представьте сообщение (реферат) согласно выбранному номеру варианта (объем сообщения не менее 2 стр. 14 Times New Roman, 1,5 интервал).

Таблица 4.1 – Варианты для выполнения практического задания

Вариант	Наименование предприятия
1	Носители информации. Виды и классификация
2	Объекты защиты на предприятии. Классификация и особенности.
3	Персонал предприятия как объект защиты.
4	Отходы производства предприятия как объект защиты.
5	Помещения предприятия как объект защиты.
6	Хранилища носителей информации как объект защиты.
7	Средства транспортировки носителей конфиденциальной информации как объект защиты.
8	Технические средства защиты информации и контроля как объект защиты.
9	Средств производства предприятия как объект защиты.

10	Средства вычислительной техники как объект защиты.
----	--

Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

Интернет-ресурсы: 1-3

Программное обеспечение: 1-2

Практическое занятие 5

Название работы: Разработка модели, технологическое и организационное построение комплексной системы защиты информации

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Теоретическая часть

Моделирование является одним из эффективных инструментов анализа сложных систем различной природы, и комплексные системы защиты в данном случае не являются исключением. Под моделью будем понимать описательно представленную систему, которая отображает объект исследования и способна замещать его так, что изучение этой системы дает адекватную информацию об объекте. Модели различаются по используемым средствам моделирования, формам и методам описания характеристик моделирования и некоторым другим критериям.

Описание объекта

Оцениваемый объект представляет собой научно-производственное предприятие, ориентированное на выпуск сложных, дорогостоящих изделий специального назначения. Предприятие обладает высоким техническим потенциалом, имеет сложное оборудование и квалифицированных специалистов. В состав предприятия входит специальное конструкторское бюро с собственной гражданской и оборонной тематикой.

В условиях резкого сокращения оборонных заказов предприятие вынуждено было начать поиск внебюджетных источников инвестиций. Одним из таких источников стало производство электрохромных активных зеркал заднего вида для легковых автомобилей, предназначенных на

свободную реализацию. Такие зеркала являются уникальными для России, обладают «ноу-хау» и имеют конкурентные преимущества высокого порядка, преодоление которых для конкурентов является сложной проблемой. Аналогичные изделия, которые поставляются в Россию, производятся еще только двумя американскими фирмами (Донелли и Гентакс). Потребителем их продукции в России является представительство фирмы Альфа-Ромео, офис которого находится рядом с центральным административным корпусом здания рассматриваемого предприятия.

Основные производственные помещения (цеха), где изготавливаются изделия, находятся в г. Чехове. Что касается представительства (центральный офис), в котором располагается руководящий аппарат, то он находится в центре Москвы. Рядом с основным корпусом административного здания находится строение, которое одновременно выполняет функции хранилища готовой продукции и выставочного комплекса.

Система защиты объекта построена по принципу выделения защищаемых зон и их декомпозиции. Внешняя зона защиты охватывает территорию от ограждения до периметра зданий (включая автостоянку).

Внутренняя зона разделена:

- ☐ на сектор защиты выделенных помещений в 1 комнату;
- ☐ сектор защиты хранилища и выставочного комплекса. Для обеспечения безопасности внешней зоны установлено металлическое ограждение высотой 3 метра.

Безопасность внутренней зоны обеспечивается следующими средствами, методами и мероприятиями:

- ☐ при входе в каждый корпус осуществляется электронный контроль. Посетители и сотрудники проходят через специальные ворота, где определяется, нет ли при них оружия и опасных предметов. Кроме того, у сотрудника проверяется пропуск, а у посетителей – документ, удостоверяющий личность;

- ☐ имеется система теленаблюдения. Сигналы с ТВ-камер выводятся на цифровые анализаторы. При срабатывании сигналов тревоги изображения с тревожных камер выводятся на видеомонитор;

- ☐ установлена система охранной сигнализации с резервным и аварийным источниками питания;

○ выделенные помещения оборудованы магнитными датчиками, реагирующими на прохождение человека с металлическим предметом достаточно большой массы;

○ применяются заранее оговоренные условные фразы и кодовые выражения при ведении телефонных разговоров по городским каналам связи о времени и месте проведения важных деловых встреч и совещаний;

○ в Устав и правила трудового распорядка, а также в контракты сотрудников внесены специальные разделы и пункты, касающиеся правил обеспечения защиты информации;

○ ежегодно проводится обучение сотрудников правилам и процедурам работы с конфиденциальной информацией;

○ определен круг лиц, которые в силу занимаемого служебного положения на предприятии имеют доступ к защищаемой информации;

○ осуществляется взаимодействие с органами внутренних дел по вопросам обеспечения безопасности;

○ в выделенных помещениях применяются звукопоглощающие облицовки и двойные оконные переплеты для защиты от прослушивания;

○ используются светонепроницаемые стекла, занавески, драпировки и другие защитные материалы для защиты от наблюдения и фотографирования.

Для защиты локально-вычислительной сети предусмотрено следующее:

○ идентификация технических средств, файлов и аутентификация пользователей; ○ регистрация и контроль работы технических средств и пользователей;

○ уничтожение информации в ЗУ после использования; ○ установлены специальные антивирусные средства; ○ ведется учет носителей.

Координирует действия по обеспечению безопасности служба защиты информации, являющаяся самостоятельным структурным подразделением.

Практическая часть Необходимо

письменно:

- ☐ представить состав основных функций и организационных элементов КСЗИ;
- ☐ объяснить, как содержательно взаимосвязаны функциональная и организационная структуры КСЗИ;
- ☐ построить и графически представить функциональную и организационную модели системы защиты информации объекта, описание которого приведено выше.

Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

Интернет-ресурсы: 1-3

Программное обеспечение: 1-2

Практическое занятие 6

Название работы: Моделирование способов физического проникновения злоумышленника к источникам информации

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Теоретическая часть

Решение проблемы защиты информации с точки зрения системного подхода можно сформулировать как трансформацию существующей системы в требуемую.

Целями системы защиты являются обеспечение требуемых уровней безопасности информации на фирме, в организации, на предприятии (в общем случае – на объекте защиты). Задачи конкретизируют цели применительно к видам и категориям защищаемой информации. А также элементам объекта защиты и отвечают на вопрос, что надо делать для достижения целей. Кроме того, уровень защиты нельзя рассматривать в качестве абсолютной меры, безотносительно от ущерба, который может

возникнуть от потери информации и использовании ее злоумышленником во вред владельцу информации.

В качестве ориентира для оценки требуемого уровня защиты информации необходимо определить соотношение между ценой защищаемой информации и затратами на ее защиту. Уровень защиты рационален, когда обеспечивается требуемый уровень безопасности информации ($C_{\text{уи}}$ $C_{\text{уд}}$) и минимизируются расходы на защиту информацию

($C_{\text{зи}}$ $C_{\text{зд}}$). Эти расходы $C_{\text{ри}}$ складываются из:

- затрат на защиту информации $C_{\text{зи}}$;
- ущерба $C_{\text{уи}}$ за счет попадания информации к злоумышленнику и использования ее во вред владельца.

Между этими слагаемыми существует достаточно сложная связь, так как ущерб из-за недостаточной безопасности информации уменьшается с увеличением расходов на ее защиту.

Если первое слагаемое может быть точно определено, то оценка ущерба в условиях скрытности разведки и неопределенности прогноза использования злоумышленником полученной информации представляет достаточно сложную задачу. Ориентировочная оценка ущерба возможна при следующих допущениях.

Владелец информации ожидает получить от ее материализации определенную прибыль, которой он может лишиться в случае попадания ее конкуренту. Кроме того, последний, используя информацию, может нанести владельцу еще дополнительный ущерб за счет, например, изменения тактики, продажи или покупки ценных бума и т.д. Дополнительные неблагоприятные факторы чрезвычайно трудно поддаются учету. Поэтому в качестве граничной меры для оценки ущерба можно использовать величину потенциальной прибыли $C_{\text{пи}}$, которую ожидает получить от информации ее владелец, т.е.

$$C_{\text{уи}} \geq C_{\text{пи}}. \quad (6.1)$$

В свою очередь величина ущерба зависит от уровня защиты, определяемой расходами на нее. Максимальный ущерб возможен при нулевых расходах на защиту, гипотетически нулевой ущерб обеспечивается при идеальной защите. Но идеальная защита требует бесконечно больших затрат.

При увеличении расходов вероятность попадания информации злоумышленнику, а, следовательно, и ущерб уменьшаются. Но одновременно увеличиваются расходы на защиту. Указанные зависимости иллюстрируются на рисунке 6.1.



Рисунок 6.1 – Зависимость расходов на информацию от затрат на ее защиту

Из рисунка 1 следует, что функция $C_{ри} = f(C_{уи}, C_{зи})$ имеет область, в которой $C_{ри}$ принимает максимальное и минимальное значения. Рост суммарных расходов на информацию с увеличением затрат на ее защиту имеет место в период создания или модернизации системы, когда происходит накопление мер и средств защиты, которые не оказывают существенного влияния на безопасность информации. Например, предотвращение утечки информации по отдельным канал без снижения вероятности утечки по всем остальным не приводит к заметному повышению безопасности информации, хотя затраты на закрытие отдельных каналов могут быть весьма существенными. Образно говоря, для объекта защиты существует определенная «критическая масса» затрат на защиту информации, при превышении которой эти затраты обеспечивают эффективную отдачу.

При некоторых рациональных затратах на защиту информации выше критических наблюдается минимум суммарных расходов на информацию. При затратах ниже рациональных увеличивается потенциальный ущерб за счет повышения вероятности попадания конфиденциальной информации к злоумышленнику, при более высоких затратах — увеличиваются прямые расходы на защиту.

Ограничения системы представляют собой выделяемые на защиту информации людские, материальные, финансовые ресурсы, а также ограничения в виде требований к системе. Суммарные ресурсы удобно выражать в денежном эквиваленте. Независимо от выделяемых на защиту информации ресурсов они не должны превышать суммарной цены защищаемой информации. Это верхний порог ресурсов.

Проектирование требуемой системы защиты проводится путем системного анализа существующей и разработки вариантов требуемой. Алгоритм этого процесса включает следующие этапы:

- определение перечня защищаемой информации, целей, задач, ограничений и показателей эффективности системы защиты;
- моделирование существующей системы и выявление ее недостатков с позиции поставленных целей и задач;
- определение и моделирование угроз безопасности информации;
- разработка вариантов (алгоритмов функционирования) проектируемой системы;
- сравнение вариантов по глобальному критерию и частным показателям, выбор наилучших вариантов;
- обоснование выбранных вариантов системы в докладной записке или в проекте для руководства организации; ○ доработка вариантов или проекта с учетом замечаний руководства.

Так как отсутствуют формальные способы синтеза системы защиты, то ее оптимизация при проектировании возможна путем постепенного приближения к рациональному варианту в результате нескольких итераций.

В ходе проектирования создаются модели объектов защиты и угроз безопасности информации, в том числе модели каналов утечки информации, оцениваются угрозы, разрабатываются способы защиты информации, выбираются технические средства, определяются эффективность защиты и необходимые затраты. Разработка способов и средств защиты информации прекращается, когда достигается требуемый уровень ее безопасности, а затраты на защиту соответствуют ресурсам.

После рассмотрения руководством предлагаемых вариантов (*лучше* двух для предоставления выбора), учета предложений и замечаний, наилучший, с точки зрения лица, принимающего решения, вариант (проект,

предложения) финансируется и реализуется путем проведения необходимых закупок материалов и оборудования, проведения строительно-монтажных работ, наладки средств защиты и сдачи в эксплуатацию системы защиты.

Следует подчеркнуть, что специалист по защите информации должен при обосновании предлагаемых руководству организации вариантов защиты учитывать психологию лица (руководителя), принимающего решение о реализации предложений, и в большинстве случаев недостаточную информированность его об угрозах безопасности информации в организации.

Психологическим фактором, сдерживающим принятие решения руководителем о выделении достаточно больших ресурсов на защиту информации является то обстоятельство, что в условиях скрытности добывания информации угрозы ее безопасности не представляются достаточно серьезными, а приобретают некоторый абстрактный характер. Знание руководителем о существовании, в принципе, таких угроз, но без достаточно убедительных доводов специалиста о наличии угроз безопасности информации в конкретной организации, не гарантирует финансирование проекта в необходимом объеме. Кроме того, руководитель в силу собственного представления об угрозах, способах и средствах их нейтрализации может преувеличивать значимость одних мер защиты и преуменьшать другие. Однако это обстоятельство не должно уменьшать энтузиазм специалиста по защите информации, так как оно характерно для любого вида деятельности, а умение обосновывать свои предложения является необходимым качеством любого специалиста.

Корректировка мер по защите информации производится после рассмотрения проекта руководством организации, а также в ходе реализации проекта и эксплуатации системы защиты.

Для защиты информации на основе системного подхода и анализа необходимо, наряду с организационным и техническим, методическое обеспечение. В соответствии с алгоритмом проектирования системы оно должно обеспечивать:

- ☐ моделирование объекта защиты;
- ☐ выявление и моделирование угроз безопасности информации;
- ☐ разработку мер инженерно-технической защиты информации.

Моделирование объектов защиты включает: ○

структурирование защищаемой информации;

○ разработку моделей объектов защиты.

Для структурирования информации в качестве исходных данных используются:

○ перечень сведений, составляющих государственную, ведомственную или коммерческую тайну; ○ перечень источников информации в организации.

Структурирование информации проводится путем классификации информации в соответствии со структурой, функциями и задачами организации с привязкой элементов информации к ее источникам. Детализацию информации целесообразно проводить до уровня, на котором элементу информации соответствует один источник.

Схема классификации разрабатывается в виде графа-структуры, нулевой (верхний) уровень иерархии которой соответствует понятию «защищаемая информация», а n-ый (нижний) – элементам информации одного источника из перечня источников организации. Основное требование к схеме классификации – общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня, т. е. одна и та же информация не должна указываться в разных элементах классификации.

Результаты структурирования оформляются в виде:

○ схемы классификации информации; ○ таблицы

6.1.

Таблица 6.1 разрабатывается на основе схемы классификации информации. В первом столбце указывается номер элемента информации в схеме классификации.

Порядковый номер элемента информации соответствует номеру тематического вопроса в структуре информации. Значность номера равна количеству уровней структуры, а каждая цифра - порядковому номеру тематического вопроса на рассматриваемом уровне среди вопросов, относящихся к одному тематическому вопросу на предыдущем уровне. Например, номер 2635 соответствует информации 5-го тематического вопроса на 4-м уровне, входящего в 3-й укрупненный вопрос 3-го уровня,

который, в свою очередь, является частью 6-го тематического вопроса 2-го уровня, представляющего собой вопрос 2-й темы 1-го уровня.

Таблица 6.1 – Классификация информации

№ элемента информации	Наименование элемента информации	Гриф конфиденциальности информации	Цена информации	Наименование источника информации	Местонахождение источника информации
1	2	3	4	5	6

Во 2-м, 3-м и 4-м столбцах таблицы указываются наименование элемента информации (тематического вопроса) и его характеристики: гриф и цена. Последующие столбцы таблицы относятся к источникам информации соответствующего ее элемента в схеме классификации. В столбце 5 указывается наименование источника (фамилия человека, название документа или его номер по книге учета, наименование и номер изделия и т.д.), а в графе 6 – места размещения или хранения (возможные рабочие места людей-источников информации, места расположения, размещения или хранения других носителей).

Эти места в общем случае представляют собой:

- ☐ помещения (служебные, лаборатории, офисы, цеха, склады, квартиры и др.);
- ☐ письменные столы рабочих мест сотрудников, хранилища и сейфы, шкафы деревянные и металлические в помещениях.

В помещениях размещается большинство источников информации: люди, документы, разрабатываемая продукция и ее элементы, средства обработки и хранения информации и др., а также источники функциональных и опасных сигналов.

Практическая часть

Вами должно быть выбран и описан конкретный объект защиты. Этим объектом может являться то предприятие, на котором вы работаете или агентство «Недвижимость» (см. информацию для описания ниже).

Таблица 6.2 - Наименование и краткое описание объекта защиты

Агентство «Недвижимость», являясь дочерней организацией агентства «Русская недвижимость», расположенного в г. Москве. В связи с расширением агентство «Недвижимость» предполагает разместиться в помещениях 2-го этажа учреждения, аналогичного помещению кафедры ОТиЗИ СГУ в аудиториях: - № 208 (разделенная на две части, в ней - 5 агентов по работе с клиентами, специалист по информационной безопасности); - № 209 (зал заседаний); - № 210 (бухгалтер и кассир); - № 211 (директор и заместитель по работе с кадрами); - холл (секретарша). Рабочие места каждого сотрудника планируется оборудовать ПЭВМ, объединенными в ЛВС с выходом в Internet. Вы – специалист по информационной безопасности.
--

Задание:

1. Необходимо предоставить детальное описание этого предприятия (объем не менее 5 страниц). Описание предприятия должно содержать следующие разделы:

☐ общее описание (где находится, чем занимается, сколько человек работает, организационная структура, структура производственных процессов и их краткое описание),

☐ нормативная база предприятия, в том числе по защите информации;

☐ план территории, расположения помещений/помещения предприятия с указанием наименований соответствующих подразделений, на плане также должны быть указаны основные конструктивные элементы помещений, расположение источников информации, средств ее обработки, линий связи, коммуникации и пр.

☐ перечень используемых информационных систем, средств и комплексов защиты.

2. Оформить результаты структурирования информации.

На основании описания предприятия необходимо произвести структурирование информации, обрабатываемой информацией. Результатом

выполнения должна быть заполненная таблица. Количество элементов информации – не менее 20.

Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

Интернет-ресурсы: 1-3

Программное обеспечение: 1-2

Практическое занятие 7

Название работы: Моделирование угроз безопасности информации

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Теоретическая часть

Обнаружение и распознавание каналов утечки информации, так же как любых объектов, производится по их демаскирующим признакам. В качестве достаточно общих признаков или индикаторов каналов утечки информации могут служить указанные в таблице 7.1.

Приведенные индикаторы являются лишь ориентирами при поиске потенциальных каналов утечки. В конкретных условиях их состав существенно больший.

Таблица 7.1 – Признаки каналов утечки информации

Вид канала	Индикаторы
Оптический	Окна, выходящие на улицу, близость к ним противоположных домов и деревьев Отсутствие на окнах занавесок, штор, жалюзей. Просматриваемость содержания документов на столах со стороны окон, дверей, шкафов в помещении Просматриваемость содержания плакатов на стенах помещения для совещания из окон и дверей. Малое расстояние между столами сотрудников в помещении Просматриваемость экранов мониторов ПЭВМ на столах сотрудников со стороны окон, дверей или других сотрудников Складирование продукции во дворе без навесов Малая высота забора и дырки в нем. Переноска и перевозка образцов продукции в открытом виде Появление возле территории организации (предприятия) посторонних людей (в том числе в автомобилях) с биноклями фотоаппаратами, кино и видеокамерами

Радиоэлектронный	Наличие в помещении радиоэлектронных средств. ПЭВМ ТА городской и внутренней АТС, громкоговорителей трансляционной сети и других предметов Выход окон помещения на улицу, близость к ним улицы и противоположных домов Применение средств радиосвязи Параллельное размещение кабелей в одном жгуте при разводке их внутри здания ч на территории организации. Отсутствие заземления радио и электрических приборов Длительная к частая парковка возле организации чужих автомобилей, в особенности с сидящими в машине людьми
Акустический	Малая толщина дверей и стен помещения
Вид канала	Индикаторы
	Наличие в помещении открытых вентиляционных отверстий Отсутствие экранов на отопительных батареях Близость окон к улице и ее домам. Появление возле организации людей с достаточно большими сумками, длинными и толстыми зонтами Частая и продолжительная парковка возле организации чужих автомобилей
Материально-вещественный	Отсутствие закрытых и опечатанных ящиков для бумаги и твердых отходов с демаскирующими веществами Применение радиоактивных веществ Неконтролируемый выброс газов с демаскирующими веществами, слив в водоемы и вывоз на свалку твердых отходов Запись сотрудниками конфиденциальной информации на неучтенных листах бумаги.

Потенциальные каналы утечки определяются для каждого источника информации, причем их количество может не ограничиваться одним или двумя. Например, от источника информации – руководителя фирмы утечка информации возможна по следующим каналам: ○ через дверь в приемную или коридор; ○ через окно на улицу или во двор:

- через вентиляционное отверстие в соседние помещения;
- с опасными сигналами по радиоканалу;
- с опасными сигналами по кабелям, выходящим из помещения; ○ по трубам отопления в другие помещения здания;
- через стены, потолок и пол в соседние помещения; ○ с помощью закладных устройств за территорию фирмы.

Потенциальные каналы утечки определяются для каждого источника информации, причем их количество может не ограничиваться одним или двумя. Например, от источника информации - руководителя фирмы утечка информации возможна по следующим каналам: ☐ через дверь в приемную или коридор; ☐ через окно на улицу или во двор:

- ☐ через вентиляционное отверстие в соседние помещения;
- ☐ с опасными сигналами по радиоканалу;
- ☐ с опасными сигналами по кабелям, выходящим из помещения; ☐ по трубам отопления в другие помещения здания;
- ☐ через стены, потолок и пол в соседние помещения;
- ☐ с помощью закладных устройств за территорию фирмы.

Все выявленные потенциальные каналы утечки информации и их характеристики записываются в таблицу 7.2.

Наименование источника информации заимствуются из таблицы 7.1. В графе 4 указываются основные элементы среды распространения и возможные места размещения приемника сигналов. По физической природе носителя определяется вид канала утечки информации.

Таблица 7.2 - Потенциальные каналы утечки информации

№ элемента Информации	Цена Информации	Источник сигнала	Путь утечки Информации	Вид канала	Оценки Реальности канала	Величина угрозы	Ранг угрозы
1	2	3	4	5	6	7	8

Оценка показателей угроз безопасности представляет достаточно сложную задачу в силу следующих обстоятельств:

- ☐ добывание информации нелегальными путями не афишируется и фактически отсутствуют или очень скудно представлены в литературе реальные статистические данные по видам угроз безопасности информации. Кроме того, следует иметь, что характер и частота реализации угроз зависят от криминогенной обстановки в районе нахождения организации и данные об угрозах,

например, в странах с развитой рыночной экономикой, не могут быть однозначно использованы для российских условий;

○ оценка угроз безопасности информации основывается на прогнозе действий органов разведки. Учитывая скрытность подготовки и проведения разведывательной операции, их прогноз приходится проводить в условиях острой информационной недостаточности;

○ многообразие способов, вариантов и условий доступа к защищаемой информации существенно затрудняют возможность выявления и оценки угроз безопасности информации. Каналы утечки информации могут распространяться на достаточно большие расстояния и включать в качестве элементов среды распространения труднодоступные места;

○ априори не известен состав, места размещения и характеристики технических средств добывания информации злоумышленника.

Оценки угроз информации в результате проникновения злоумышленника к источнику или ее утечки по техническому каналу проводятся с учетом меры (вероятности) P_p реализуемости «рассматриваемого пути или канала, а также цены соответствующего элемента информации $C_{ин}$.

Угроза безопасности информации, выраженной в величине ущерба $C_{уи}$ от попадания ее к злоумышленнику, определяется для каждого пути или канала в виде $C_{уи} = C_{ин} * P_p$.

Моделирование угроз безопасности информации завершается их ранжированием в таблицах 7.1 и 7.2.

На каждый потенциальный способ проникновения злоумышленника к источнику информации и канал утечки информации целесообразно завести карточку, в которую заносятся в табличной форме характеристики моделей канала. Структурная, пространственная, функциональная и информационная модели являются приложениями к комплексной модели канала утечки. На этапе разработки способов и средств предотвращения проникновения злоумышленника и утечки информации по рассматриваемому каналу к карточке добавляется приложение с перечнем мер по защите и оценками затрат на нее.

Более удобным вариантом является представление моделей на основе машинных баз данных, математическое обеспечение которых позволяет учесть связи между разными моделями, быстро корректировать данные в них и систематизировать каналы по различным признакам, например, по виду, положению в пространстве, способам и средствам защиты, угрозам.

Практическая часть

Задание:

1. Определить возможные каналы утечки информации для защищаемого объекта.
2. Результаты анализа занести в таблицу 5. Указать не менее 10 технических каналов утечки.
3. Графически изобразите на плане предприятия выявленные технические каналы утечки информации.

Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

Интернет-ресурсы: 1-3

Программное обеспечение: 1-2

Практическое занятие 8

Название работы: Разработка организационных и технических мер по инженернотехнической защите информации

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Теоретическая часть

Так как не существует формальных методов синтеза вариантов предотвращения угроз безопасности информации, то разработка мер по защите информации проводится эвристическим путем на основе знаний и опыта соответствующих специалистов. Однако в интересах минимизации ошибок процесс разработки должен соответствовать следующим рекомендациям.

Разработку мер защиты информации целесообразно начинать с угроз, имеющих максимальное значение, далее - с меньшей угрозой и так далее до тех пор, пока не будут исчерпаны выделенные ресурсы. Такой подход гарантирует, что даже при малых ресурсах хватит средств для предотвращения наиболее значимых угроз. Для каждой угрозы разрабатываются меры (способы и средства) по защите информации. Перечень типовых способов и средств приведены в таблице 8.1.

Таблица 8.1 - Перечень типовых способов и средств

Способы реализации угроз	Типовые способы и средства предотвращения угроз
Физический контакт злоумышленника с источником информации	Механические преграды (заборы, КПП, двери, взломостойкие стекла, решетки на окнах, хранилища, сейфы), технические средства охраны, телевизионные средства наблюдения, дежурное и охранное освещение, силы и средства нейтрализации угроз.
Воздействие огня	Технические средства пожарной сигнализации, средства пожаротушения - огнестойкие хранилища и сейфы.
Наблюдение	Маскировочное окрашивание, естественные и искусственные маски, ложные объекты, аэрозоли, пены, радиолокационные отражатели, радио- и звукопоглощающие покрытия, тепло-изолирующие материалы, генераторы радио- и гидроакустических помех.
Подслушивание	Скремблирование и цифровое шифрование, звукоизолирующие конструкции, звукоизолирующие

	материалы, акустическое и вибрационное зашумление, обнаружение, изъятие и разрушение закладных устройств.
Способы реализации угроз	Типовые способы и средства предотвращения угроз
Перехват	Выполнение требований по регламенту и дисциплине связи, отключение источников опасных сигналов, фильтрация и ограничение опасных сигналов, применение буферных устройств, экранирование, пространственное и линейное зашумление.
Утечка информации по материально-вещественному каналу	Учет и контролируемое уничтожение черновиков, макетов, брака, сбор и очистка от демаскирующих веществ отходов.

Так как меры по защите информации рассматриваются для каждой угрозы, то в контролируемой зоне возможно их дублирование. Например, полу-открывая дверь в служебное помещение может способствовать как наблюдению документов и экранов ПЭВМ в помещении, так и подслушиванию ведущихся в нем разговоров. Установленные на дверь устройство для автоматического ее закрытия и кодовый замок предотвращают утечку информации по этим каналам.

Следовательно, разработка мер по предотвращению угроз представляет собой итерационный процесс, каждая итерация которого выполняется в 2 этапа:

- разработка локальных мер по предотвращению каждой из выявленных угроз;
- интеграция (объединение) локальных мер. Условием для перехода к следующей итерации является освобождение в результате объединения способов и средств защиты информации части ресурса. достаточно и "для предотвращения очередной угрозы.

Рекомендуемые способы и средства защиты информации заносятся в таблицу, вариант которой приведен в таблице 8.2.

Таблица 8.2 – Рекомендуемые способы и средства защиты

№ элемента информации	Тип угрозы	Величина угрозы	Способы предотвращения угроз	Средства предотвращения угроз	Затраты на предотвращения угроз
1	2	3	4	5	6
Суммарные затраты на защиту информации					

Практическая часть

Игровая ситуация – агентство «Недвижимость».

Задание:

1. Проанализировать угрозы, начиная с угроз, имеющих максимальное значение, далее - с меньшей угрозой и так далее до тех пор, пока не будут исчерпаны выделенные ресурсы.
2. Принять решение по инженерно-технической защите охраняемого объекта, результаты оформить таблицей 2.

Список литературы, рекомендуемый к использованию по данной теме.

Основная литература: 1-3

Дополнительная литература: 1-6

Интернет-ресурсы: 1-3

Программное обеспечение: 1-2

Практическое занятие 9

Название работы: Система контроля и управления доступом

Формируемые компетенции: ОПК-10, ОПК-2.2, ОПК-2.3, ОПК-2.4.

Цели:

- ☐ Закрепить теоретические знания
- ☐ Изучить методы оценки эффективности системы контроля и управления доступом

Подготовка к работе

При домашней подготовке лабораторной работы необходимо подготовить отчет, содержащий:

- ☐ титульный лист с указанием ФИО, специальности, группы и курса;
- ☐ основные теоретические сведения;
- ☐ порядок и результаты расчётов при выполнении заданий;
- ☐ выводы.

Ход занятия

1. Проверка готовности студентов к занятию.
2. Проверка знаний теоретического материала и порядка выполнения заданий.
3. Выполнение заданий практического занятия.
4. Составление отчета.

Теоретическая часть

На сегодняшний день существует несколько методических подходов к оценке эффективности системы контроля и управления доступом (СКУД).

Рассмотрим следующие из них:

1. Детерминистический подход.
2. Логико-вероятностные методы.
3. Вероятностно-временной анализ.
4. Методы многокритериальной оптимизации.

5. Имитационное моделирование.

1. Детерминистический подход

Детерминистический подход к оценке эффективности СКУД связан с заданием и последующей проверкой обязательных требований, содержащихся в ведомственных руководящих документах, ТЗ на проектирование, рабочем проекте. Этот подход предполагает проведение комплексных проверок (инспекций), например, органами государственного надзора или ведомственного контроля. Такие проверки могут проводиться с различной регулярностью (плановые проверки), а кроме того – при изменении перечня угроз объекту, модернизации СКУД и в ряде других случаев (внеплановые проверки). Контролю при этом подвергаются организационные мероприятия, комплекс инженерно-технических средств охраны, действия персонала службы безопасности. Для этого разрабатываются опросные листы, содержащие формализованные перечни требований по организации доступа на объекте, в том числе по оснащению периметра объекта, его зданий, сооружений инженерно-техническими средствами охраны, по оценке состояния личного состава службы безопасности, по наличию и качеству проводимых организационных мероприятий. По своему характеру этот метод является экспертным. Процедура экспертного оценивания может быть построена по-разному. В одних случаях результаты могут интерпретироваться на качественном уровне, в других, на основании полученных данных, могут конструироваться интегральные критерии, отражающие состояние СКУД объекта в целом. В качестве конкретной реализации данного подхода рассмотрим разработанный в Госатомнадзоре экспертный метод оценки состояния физической защиты (РД-07-01-2004 «Методические указания по проведению оценки состояния физической защиты ядерно- и радиационноопасных объектов по результатам проведенной инспекции»). Целями оценки состояния являются:

- проверка соответствия физической защиты предъявляемым к ней требованиям;
- выявление элементов, не соответствующих требованиям к физической защите (т.н. «критических элементов» СКУД).

Для этого разработана целая система факторов состояния (ФС), которые определяют организацию и обеспечение физической защиты в соответствии с требованиями нормативных документов. В том числе различают:

- ФС организационных мероприятий (группа а);
- ФС инженерно-технических средств охраны (группа b); –
- ФС действий подразделений охраны (группа с).

Процедура оценки следующая:

1. Эксперт выбирает некоторое количество ФС по группам а, b, с соответственно. Каждому ФС каждый эксперт назначает определенный «вес».

2. Каждому ФС эксперты дают оценку степени реального состояния ФС ($d_{ij} = 0, 1, 2, 3$).

3. Определяется среднее значение показателя реального состояния каждого ФС d_i :

$$d_i = \frac{\sum_{j=1}^n d_{ij}}{n} \quad (9.1)$$

где d_{ij} – показатель реального состояния i -го ФС, назначенного j -м экспертом; n – число экспертов.

4. Состояние СКУД объекта в целом оценивается следующим образом (табл. 1):

○ члены комиссии определяют значения средних весов ФС a_i, b_i, c_i аналогично d_i ;

○ определяются показатели состояния составных частей физической защиты N_1, N_2, N_3 ;

○ за показатель состояния физической защиты принимается среднее арифметическое значений N_1, N_2, N_3 .

Таблица 9.1 – Оценки показателей состояния составных частей СКУД

Показатель состояния:	Формула для его оценки:
-----------------------	-------------------------

– организационных мероприятий	$\begin{array}{c} \star^k \quad a \quad d \\ N_1 \textcircled{P} \quad i \textcircled{P} 1 \quad i \\ d_m k a_m \end{array}$
– инженерно-технических средств	$\begin{array}{c} \star^l \quad b \quad d \\ N_2 \textcircled{P} \quad i \textcircled{P} 1 \quad i \\ d_m l b_m \end{array}$
– действий подразделений охраны	$\begin{array}{c} \star^m \quad c \quad d \\ N_3 \textcircled{P} \quad i \textcircled{P} 1 \quad i \\ d_m m c_m \end{array}$
k – число ФС в организационных мероприятиях; l – число ФС в инженерно-технических средствах ФЗ; m – число ФС в действиях подразделений охраны; d_m – максимально возможное значение показателя реального состояния ФС ($d_m = 3$); a_m, b_m, c_m – максимально возможные значения весов ФС в группе ФС (5, 6, 4 соответственно).	

Интерпретация результатов оценки приведена в таблице 9.2.

Таблица 9.2 – Интерпретация результатов оценки состояния физической защиты

Значение показателя состояния N:	Соответствие ФЗ требованиям:
$N \leq 0,05$	ФЗ в основном соответствует требованиям норм и правил
$0,05 < N < 0,07$	ФЗ имеет отдельные отступления от требований норм и правил
$0,07 < N < 0,1$	Имеет значительные отступления от требований норм и правил, требующие использования компенсирующих мероприятий
$N \geq 0,1$	ФЗ не обеспечивается

3. С помощью данного метода можно судить, насколько полно выполняются требования к СКУД на конкретном объекте. Однако он не позволяет учитывать такие факторы, как правильность установки и

настройки технических средств охраны, просчеты в применении сил охраны объекта и др. Свою роль может сыграть и недостаточная компетентность экспертов. Поэтому даже отвечающая всем требованиям СКУД в реальных условиях может оказаться неспособной решать поставленные перед ней задачи.

2. Логико-вероятностные методы

Большие потенциальные возможности для оценки эффективности функционирования СКУД содержат в себе логико-вероятностные методы (ЛВМ). Эти методы давно применяются в отечественной практике для анализа живучести, надежности и безопасности структурно- и качественно-сложных систем. Теоретическую основу ЛВМ составляют операции над функциями булевой алгебры. При расчете надежности исследуются условия нахождения системы в работоспособном состоянии, а при анализе безопасности – условия попадания системы в опасное состояние. Целью исследования является определение степени риска, присутствующего в системе. Пусть y – логическая функция, описывающая функционирование СКУД. Степень риска $y(y)$ – вероятностная величина, характеризующая возможность невыполнения СКУД своей целевой функции в рамках конкретной проектной угрозы. Структура СКУД описывается при помощи функций алгебры логики, а количественная оценка степени риска проводится с помощью теории вероятности.

Процедура оценки выглядит следующим образом:

1. Составляется сценарий развития опасности, представляющий собой логико-вероятностную модель функционирования СКУД. Сценарий представляется в виде графа (типа «дерева») и содержит события трех видов: иницирующие, промежуточные, конечное. Иницирующие события описывают воздействия нарушителя на систему (преодоление периметра объекта, имитация процедуры идентификации на КПП и др.). Промежуточные события получаются путем логической комбинации двух или более событий (конъюнкция, дизъюнкция событий и др.). Конечное событие описывает определенное опасное состояние системы (например, проникновение нарушителя к цели акции раньше сил быстрого реагирования).

Составление сценария – творческая задача. От того, насколько полно будет описана схема функционирования СКУД, учтены причинноследственные связи между событиями, зависит достоверность результатов анализа.

2. Составляется функция опасности системы $y(z_1..z_n)$, ее аргументами являются инициирующие события, а значением – конечное (опасное) событие.

3. Функция опасности системы заменяется вероятностной функцией $P\{y(z_1..z_m)\}$ следующим образом:

- z_i заменяется на $P\{z_i = 1\} = R_i$ (вероятность того, что i -е инициирующее событие произойдет);
- z_i' заменяется на $P\{z_i' = 1\} = Q_i = 1 - R_i$. (вероятность того, что i -е инициирующее событие не произойдет).

4. Ищется значение вероятностной функции в предположении реализации опасного события:

$$Y(y) = P\{y(z_1..z_m) = 1\}. \quad (9.2)$$

Эта формула и определяет степень риска, присутствующего в системе.

Недостатком этого метода является значительный объем трудоемких логических преобразований при анализе сложных сценариев (переход от функции опасного состояния к вероятностной функции). Для автоматизации расчетов разработан и используется целый ряд компьютерных программ, в том числе Relex (США), Risk Spectrum (Швеция), «Арбитр» (ПК «АСМ») (Россия).

1. Метод дает обоснованный количественный показатель эффективности СКУД. Можно рассматривать анализ безопасности как метод многокритериальной оптимизации.

2. С помощью данного метода можно построить модель безопасного функционирования СКУД, определить «уязвимые места» системы и проранжировать их по степени безопасности.

3. Применение ЛВМ позволяет выявить внутреннюю структуру СКУД, придав ей черты структурно простой или структурно сложной системы.

4. Недостатками данного метода являются трудоемкость логиковеероятностных преобразований, а также проблема достоверности вероятностей инициирующих событий.

3. Вероятностно-временной анализ

Основной метод, используемый в настоящее время для оценки эффективности СКУД. Принципы вероятностно-временного анализа были разработаны в конце 70-х годов в Сандийских национальных лабораториях (США) для использования при оценке эффективности физической защиты объектов Департамента энергетики США, а также других важных государственных объектов.

Эффективность СКУД рассматривается здесь как вероятностная величина: вероятность того, что силы охраны, действующие по сигналам технических средств охраны, успеют пресечь акцию нарушителя. Суть метода состоит в следующем.

Для пресечения акции внешнего нарушителя проверяется выполнение условия $DT = T_o - T_n < 0$ для конкретной оперативной ситуации. Для этого анализируются маршруты движения нарушителей и сил охраны для каждой из целей, определенных на этапе анализа уязвимости. Оцениваются времена движения t_{i_n} и t_{i_o} , относящиеся к различным этапам их действий. Для нарушителя это могут быть время преодоления физических барьеров, время движения по территории объекта, время акции и т.д., для охраны – время сборов, время движения, время осмотра «сработавшего» участка периметра и др. Понятно, что эти времена являются случайными. Более того, законы их распределения неизвестны. Однако, если t_i независимы и количество этапов l достаточно велико, то в соответствии с центральной предельной теоремой их сумма

$$T \textcircled{P} \star_{l \textcircled{P} 1 t_i} \quad (9.3) \text{ оказывается распределена по нормальному}$$

закону. Это значит, что:

$$M \sqrt{T} \textcircled{P} \star_{l \textcircled{P} 1} M \sqrt{t_i} \textcircled{P} \quad (9.4)$$

○ математическое ожидание времен сил охраны и нарушителя;

$$D \sqrt{T} \textcircled{P} \star_{l \textcircled{P} 1} D \sqrt{t_i} \textcircled{P} \quad (9.5)$$

○ дисперсия времен сил охраны и нарушителя.

По тому же закону оказывается распределенным резерв времени сил охраны: $P(\Delta T < 0)$. Этой идее можно придать наглядную геометрическую трактовку (рис. 1). Вероятность того, что силы охраны успеют перехватить нарушителя $P_{\text{пер}} = P(T_o < T_n)$, выражается площадью под кривыми $f(T_o)$ и $f(T_n)$ (рис. 1), где $f(T_o)$, $f(T_n)$ – плотности распределения вероятностей времен T_o и T_n соответственно.

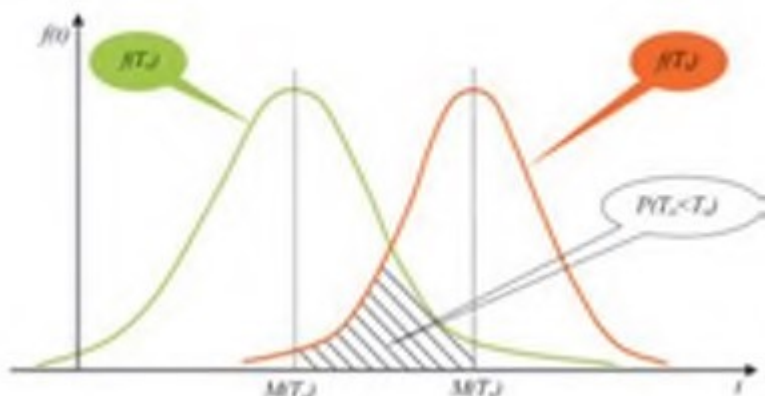


Рисунок 9.1 – Графическая трактовка вероятности $P(T_{\text{он}})$ пресечения действий нарушителя в СКУД

Таким образом определяются дифференциальные показатели эффективности. Для формирования интегрального показателя эффективности могут применяться различные методы агрегирования информации, подобные тем, что описаны выше, с присвоением «веса» каждой угрозе.

1. Достоинством данного метода является обоснованность взвешенного суммирования дифференциальных показателей, вытекающая из однородности их физической природы.

2. Объективность и достоверность результатов оценки сильно зависят от точности исходных данных по вероятностям обнаружения нарушителя техническими средствами, временам движения охраны и нарушителя, временам преодоления физических барьеров и т.д. Вообще, априорная неопределенность исходных данных, часть из которых имеет характер экспертного оценивания, требует достаточно осторожного отношения к результатам расчетов и их интерпретации.

3. Другим недостатком этого метода является значительный объем рутинных вычислительных процедур при анализе СКУД на реальных объектах.

Вообще говоря, реализовать описанный выше «ручной» алгоритм оценки удастся только для простейших объектов. Для объектов со сложной конфигурацией охраняемых зон, множеством целей и маршрутов движения нарушителей оценка может быть произведена только с использованием специализированных компьютерных программ. В настоящее время разработаны и используются несколько программных средств для оценки эффективности СКУД, в том числе EASI (Estimate of Adversary Sequence Interruption), ASSESS (Analytic System and Software for Evaluating Safeguards and Security) («Сандийские национальные лаборатории», США), программный комплекс «СПРУТ» (НПП «ИСТА-Системс», Россия).

4. Методы многокритериальной оптимизации

Основой данных методов является агрегирование информации о частных показателях качества. Среди них выделяют методы лексикографического упорядочивания, итерационные методы предпочтительного выбора, аксиоматический подход с использованием теории полезности и пр.

Рассмотрим, например, один из итерационных методов – метод "смещенного идеала". Пусть задано n объектов, оцененных по m критериям: $k_1 \dots k_m$. Процедура оптимизации такова:

1. Моделируются два многокритериальных объекта (МКО): "условно предпочтительный", формируемый из максимальных по полезности значений критериев $MKO' \oplus k_1' \dots k_m'$ и наихудший – из минимальных по полезности значений критериев: $MKO \oplus k_1 \dots k_m$.

2. Задается вектор предпочтений, например $W_1 \oplus \langle 4, 3, 3, 2 \rangle$. Он отражает предпочтения лица, принимающего решение в отношении оптимизируемых показателей эффективности.

3. Чтобы выявить объекты, которые не претендуют на предпочтительные, их сравнивают с идеальным, вычисляя "расстояние" (метрику) до идеального. Так, объекты ранжируются по расстоянию от идеального объекта, например: $B_1 \oslash B_4 \oslash B_2 \oslash B_3$. Наименее предпочтительный

объект B_3 исключается из рассмотрения, после чего процедура повторяется. Таким образом, исключая неподходящие объекты, в конце остается один, наиболее предпочтительный.

5. Имитационное моделирование

Вероятностный подход к анализу базируется на предположениях о случайности и независимости временных параметров в системе "охрананарушитель". Эффективность здесь понимается как вероятность пресечения несанкционированных действий нарушителя:

$P_{\text{ПРЕС}} \oplus P_{\text{ОБН}} * P_{\text{НЕЙТР}}$, где $P_{\text{ОБН}}$ - вероятность обнаружения нарушителя; $P_{\text{НЕЙТР}}$ - вероятность нейтрализации нарушителя.

Как оценить эти вероятности? Один из методов - имитационное моделирование. Это вычислительный эксперимент, основанный на том известном факте, что при увеличении числа испытаний n относительная частота $W \oplus m/m$ появления случайного события A в серии испытаний стремится к его вероятности в единичном испытании $W_{p>A}$ при $n \rightarrow \infty$. С помощью генератора случайных чисел получают выборки случайных величин, распределенных по известному закону с известными математическим ожиданием и дисперсией. Приведем пример. Периметр объекта оборудован системой охранной сигнализации с вероятностью обнаружения $P_{\text{ОБН}} \oplus 0,95$. Для имитационного моделирования работы такой системы "разыгрывается" равномерно распределенное случайное число k от 0 до 1. Если $k \leq 0,95$, система сработала, в противном случае - нет. Таким же образом моделируется время движения сил охраны и нарушителя и другие случайные процессы в функционировании СКУД.

Каждая конфликтная ситуация в функционировании СКУД просчитывается много раз, по результатам набирается статистика захватов нарушителя. Эффективность СКУД оценивается статистически, как отношение числа захватов к общему числу испытаний. Количество опытов определяется исходя из того, что при заданной доверительной вероятности необходимо обеспечить требуемую точность оценки.

ЗАКЛЮЧЕНИЕ

Таковы в кратком изложении основные методы, используемые на сегодняшний день для оценки эффективности СКУД. Разумеется, они появились не сегодня. В 2003 году на русском языке вышла книга М. Гарсиа «Проектирование и оценка систем физической защиты» (Пер. с англ. – М.: «Мир», 2003), где был обобщен опыт американских специалистов в этой области. Первой отечественной книгой, в которой в связном виде изложены основные методические подходы к оценке эффективности СКУД, является издание А.В. Бояринцева, А.Н. Бражника, А.Г. Зуева «Проблемы антитерроризма: Категорирование и анализ уязвимости объектов» (СПб.: ЗАО «НПП «ИСТА-Системс», 2006).

Важно понимать, что не существует универсального определения «эффективности», это следует, в частности, из множественности описания СКУД как сложной технической системы. Содержательная трактовка этого понятия зависит от используемой методологии, каждая из которых обладает своими достоинствами и недостатками. Так, при детерминистическом подходе эффективность понимается как степень выполнения требований по физической защите объекта и оценивается экспертным путем. В логиковеероятностных моделях эффективность формулируется как вероятность нахождения системы в безопасном состоянии в рамках построенного сценария развития опасности. При вероятностно-временном анализе под эффективностью понимается вероятность того, что резерв времени сил охраны окажется больше нуля $P(T_o - T_n > 0)$.

Достоинством детерминистического подхода является то, что в руки проектировщика даются четкие и ясные критерии того, как оборудовать объект техническими средствами охраны. Основная проблема – способ получения интегрального показателя. Наиболее распространена "линейная свертка" вида: $K \oplus \star a_i \odot k_i$ – экспертная оценка частного показателя, a_i – "вес" показателя). Необходимо помнить, что операция осреднения имеет смысл, если частные показатели однотипны, то есть имеют одинаковую "физическую природу". Если это не так, такой интегральный показатель не имеет физического смысла.

Достоинством имитационного моделирования является физически обоснованный критерий эффективности (вероятность). Недостаток - трудность его интерпретации и нормирования. Пусть в результате анализа

получено значение $P_{ПРЕС} \textcircled{P} 0,9$. Не ясно, много это или мало, достаточен уровень защиты объекта или нет?

В результате использования логико-вероятностных методов для анализа эффективности тоже получается число $k_{\text{риск}} \langle y \rangle$. Но смысл здесь не в цифре, а в том, что логико-вероятностное моделирование позволяет построить модель безопасного функционирования СКУД, определить "уязвимые места" системы и оценить "вклад" каждого из них, ранжируя их по степени опасности. В качестве недостатков здесь можно отметить трудоемкость логических преобразований при анализе сложных сценариев (переход от функции опасного состояния к вероятностной функции), а также разнородность исходных данных (объективных, которые можно достоверно оценить, и субъективных, отражающих "ожидания угрозы").

Между этими трактовками нет непреодолимой пропасти. По существу, это разные взгляды на одно и то же явление.

Важно то, что в руки аналитику дается набор инструментов, пригодных для научного анализа и синтеза СКУД.

Практическая часть Задание

1:

Оцените эффективность СКУД на основе детерминистического подхода, используя данные, приведённые ниже. Сделайте вывод о соответствии физической защиты требованиям норм и правил согласно таблице 2.

ФС организационных мероприятий

1. Наличие инструкций на все возможные нештатные ситуации при функционировании СКУД
2. Обученность сотрудников охраны действиям при нарушении контрольно-пропускного режима
3. Регулярное обновление модели угроз и модели нарушителя
4. Организация отлаженной системы выдачи, смены и отзыва пропусков
5. Знание сотрудниками организации регламента по получению доступа в различные помещения предприятия

ФС инженерно-технических средств охраны

1. Наличие ограды территории
 2. Наличие контрольно-пропускных пунктов для автотранспорта и персонала
 3. Наличие системы обнаружения попытки несанкционированного доступа на территорию предприятия
 4. Наличие системы видеонаблюдения
 5. Наличие единой компьютерной базы данных пропусков и времени посещения территории предприятия
 6. Наличие на территории предприятия зон с различным уровнем допуска
- ФС действий подразделений охраны
1. Своевременное реагирование на сигналы тревоги
 2. Организация непрерывного посменного дежурства на постах охраны
 3. Неукоснительное соблюдение всех инструкций по реагированию на нештатные ситуации
 4. Разъяснение персоналу предприятия и посетителям особенностей доступа на территорию предприятия и в его различные зоны

Таблица 9.3 – Экспертная оценка степени реального состояния ФС организационных мероприятий

Эксперты	ФС организационных мероприятий				
	1	2	3	4	5
Эксп. 1	3	2	0	3	1
Эксп. 2	2	2	0	2	2
Эксп. 3	3	3	0	3	2
Эксп. 4	1	3	1	3	1

Таблица 9.4 – Экспертная оценка "веса" ФС организационных мероприятий

Эксперты	ФС организационных мероприятий				
	1	2	3	4	5

Эксп. 1	5	2	1	4	3
Эксп. 2	5	4	1	2	3
Эксп. 3	4	3	2	1	5
Эксп. 4	3	4	1	2	5

Таблица 9.5 – Экспертная оценка степени реального состояния ФС инженерно-технических средств охраны

Эксперты	ФС инженерно-технических средств охраны					
	1	2	3	4	5	6
Эксп. 1	1	1	2	3	1	3
Эксп. 2	1	2	2	2	2	2
Эксп. 3	2	1	3	3	2	2
Эксп. 4	1	1	1	2	1	2

Таблица 9.6 – Экспертная оценка "веса" ФС инженерно-технических средств охраны

Эксперты	ФС инженерно-технических средств охраны					
	1	2	3	4	5	6
Эксп. 1	1	2	4	5	3	6
Эксп. 2	2	1	4	6	3	5
Эксп. 3	1	2	5	6	4	3
Эксп. 4	1	3	6	5	4	2

Таблица 9.7 – Экспертная оценка степени реального состояния ФС действий подразделений охраны

Эксперты	ФС действий подразделений охраны			
	1	2	3	4
Эксп. 1	2	2	2	2
Эксп. 2	1	2	2	3
Эксп. 3	2	3	3	0
Эксп. 4	1	3	3	1

Таблица 9.8 – Экспертная оценка "веса" ФС действий подразделений охраны

Эксперты	ФС действий подразделений охраны			
	1	2	3	4
Эксп. 1	1	3	2	4
Эксп. 2	2	3	1	4
Эксп. 3	2	4	1	3
Эксп. 4	1	4	2	3

Задание 2

Используя метод имитационного моделирования, оцените эффективность охраны объекта для следующих ситуаций:

1. Несанкционированное проникновение на внутренний двор предприятия с целью похищения пропусков из автомашины.
2. Несанкционированное проникновение в производственный цех предприятия с целью кражи образцов продукции.
3. Несанкционированное проникновение в кабинет финансового директора предприятия с целью кражи договоров о поставщиках. Для доступа в кабинет необходимо пройти по коридору здания.
4. Санкционированное проникновение во внутренний двор предприятия с последующим несанкционированным проникновением в кабинет генерального директора с целью кражи правоустанавливающих документов.

Таблица 9.9 – Вероятность обнаружения преодоления рубежей охраны

Рубеж охраны	Вероятность обнаружения преодоления рубежа, $P_{обн}$
Ограда территории	0,86
Внутренний двор	0,9
Производственный цех	0,5
Коридор здания управления	0,93
Кабинет финансового директора	0,95

Кабинет генерального директора	0,97
Контрольно-пропускной пункт	0,99

Таблица 9.10 – Вероятность пресечения несанкционированного доступа на рубеже охраны

Рубеж охраны	Вероятность пресечения НСД на рубеже, $P_{\text{прес}}$
Ограда территории	0,2
Внутренний двор	0,5
Производственный цех	0,3
Коридор здания управления	0,7
Кабинет финансового директора	0,9
Кабинет генерального директора	0,95
Контрольно-пропускной пункт	0,99

Список использованных источников

Книги с различным количеством авторов:

1. Гарсиа М. Проектирование и оценка систем физической защиты. - М.: Мир, 2003.
2. Бояринцева А.В., Бражника А.Н., Зуева А.Г. Проблемы антитерроризма: Категорирование и анализ уязвимости объектов. - СПб.: ЗАО «НПП «ИСТА-Системс», 2006.
3. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В., Скрыль С.В., Голубятников И.В. Технические средства и методы защиты информации. – М.: Машиностроение, 2009. – 508 с.

Статьи из журналов и периодических сборников, продолжающихся сборников, ежегодников:

4. Журнал «БДИ» №3, май-июнь, 2007. С. 22-27.

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

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для обучающихся по организации и проведению самостоятельной работы по
дисциплине «Комплексная система защиты информации на предприятии»

для студентов направления подготовки

10.03.01 «Информационная безопасность» Направленность
(профиль):

«Организация и технологии защиты информации (по отрасли или в сфере
профессиональной деятельности)»

Ставрополь

2026

174

СОДЕРЖАНИЕ

Введение	
1. Общая характеристика самостоятельной работы студента	2.
Технологическая карта самостоятельной работы студента.....	
3. Самостоятельное изучение тем лекций	
4. Паспорт фонда оценочных средств для проверки самостоятельной работы	
5. Список рекомендуемой литературы	

ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ:

1. дать основы сущности, целей и задач комплексной системы защиты информации, принципов и этапов ее разработки;
2. освоить технологии установления состава защищаемой информации и объектов защиты, получить необходимые знания по методам оценки уязвимости защищаемой информации;
3. научиться определять параметры и структуру комплексной системы защиты информации, проведению мероприятий по обеспечению функционирования комплексной системы защиты информации;
4. познакомить со структурой и методами управления комплексной системой защиты информации, подходами к определению показателей эффективности и методиками ее оценки.

1. Общая характеристика самостоятельной работы студента

Основными видами учебной работы по достижению результатов освоения дисциплины являются лекции, лабораторные работы и практические занятия и самостоятельная работа студентов (СРС).

На лекциях раскрываются основные положения и понятия курса, формируются знания в области комплексной системы защиты информации на предприятии. На лабораторных работах и практических занятиях формируются умения и навыки, необходимые для решения задач профессиональной деятельности.

Приступая к изучению учебной дисциплины, необходимо ознакомиться с учебной программой, получить в библиотеке рекомендованные учебные пособия, а также получить у ведущего преподавателя в электронном виде конспекты лекций, методические рекомендации к лабораторным работам и тестовые, завести новую тетрадь для конспектирования лекций и выполнения лабораторных работ и практических занятий.

Для изучения дисциплины предлагается список основной и дополнительной литературы. Основная литература предназначена для обязательного изучения, дополнительная – поможет более глубоко освоить отдельные вопросы, подготовить исследовательские задания и выполнить задания для самостоятельной работы.

В ходе лекционных занятий студент обязан осуществлять конспектирование учебного материала, особое внимание, обращая на категории, формулировки, раскрывающие содержание тех или иных понятий, физических явлений, процессов, эффектов. В рабочих конспектах желательно оставлять поля, на которых следует делать пометки из рекомендованной литературы, дополнять материал прослушанной лекции,

формулировать научные выводы и практические рекомендации. Студент имеет право задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Самостоятельная работа студентов над материалом учебной дисциплины является неотъемлемой частью учебного процесса и должна предполагать углубление знания учебного материала, излагаемого на аудиторных занятиях, и приобретение дополнительных знаний по отдельным вопросам самостоятельно.

Основными видами самостоятельной работы курсантов по учебной дисциплине являются:

- ☐ самостоятельное изучение учебного материала по заданным темам;
- ☐ подготовка к лабораторным работам, оформление отчета по выполненному практическому занятию и лабораторной работе и подготовка к собеседованию по результатам работы.

Основными методами самостоятельной работы студентов являются: 1)

для овладения знаниями:

- ☐ чтение текста (конспекта лекций, учебника, дополнительной литературы) и конспектирование текста;
- ☐ работа с нормативными документами;
- ☐ поиск информации в Интернет;

2) для закрепления и систематизации знаний:

- ☐ работа с конспектом лекции (обработка текста);
- ☐ повторная работа над учебным материалом (учебника, дополнительной литературы, слайдами);
- ☐ составление плана и тезисов ответа или графическое изображение структуры ответа;
- ☐ составление таблиц для систематизации учебного материала;
- ☐ изучение нормативных документов;
- ☐ ответы на контрольные вопросы; 3) для формирования умений:
- ☐ подготовка к практическим занятиям и лабораторным работам;
- ☐ решение задач и практических заданий лабораторных работ;
- ☐ подготовка отчетов по практическим занятиям и лабораторным работам; ☐ рефлексивный анализ профессиональных умений.

В случае пропуска учебного занятия студент может воспользоваться содержанием различных блоков учебно-методического комплекса (лекции, практические и лабораторные занятия, контрольные вопросы и тесты) для самоподготовки и освоения темы. Для самоконтроля необходимо использовать вопросы и задания, предлагаемые к практическим занятиям, лабораторным работам, а также варианты тестовых заданий.

2. Технологическая карта самостоятельной работы студента

			Объем часов, в том числе
--	--	--	--------------------------

Коды реализуемых компетенций, индикатора(ов)	Вид деятельности студентов	Средства и технологии оценки	СРС	Контактная работа с преподавателем	Всего
7 семестр					
ОПК-10 ИД-1 ОПК-10 ИД-2 ОПК-10 ИД-3 ОПК-2.2 ИД-1 ОПК-2.2 ИД-2 ОПК-2.3 ИД-3 ОПК-2.3 ИД-4 ОПК-2.4 ИД-3 ОПК-2.4 ИД-4	Подготовка к лабораторной работе	Собеседование	7.85	0.25	8.1
ОПК-10 ИД-1 ОПК-10 ИД-2 ОПК-10 ИД-3 ОПК-2.2 ИД-1 ОПК-2.2 ИД-2 ОПК-2.3 ИД-3 ОПК-2.3 ИД-4 ОПК-2.4 ИД-3 ОПК-2.4 ИД-4	Подготовка к лекции	Конспект	7.85	0.25	8.1
ОПК-10 ИД-1 ОПК-10 ИД-2 ОПК-2.2 ИД-1 ОПК-2.2 ИД-2 ОПК-2.3 ИД-3 ОПК-2.3 ИД-4 ОПК-2.4 ИД-3 ОПК-2.4 ИД-4	Подготовка к практическому занятию	Собеседование	7.85	0.25	8.1
ОПК-10 ИД-1 ОПК-10 ИД-2 ОПК-10 ИД-3 ОПК-2.2 ИД-1 ОПК-2.2 ИД-2 ОПК-2.3 ИД-3 ОПК-2.3 ИД-4	Самостоятельное изучение литературы	Конспект	7.85	0.25	8.1
ОПК-2.4 ИД-3 ОПК-2.4 ИД-4					

ОПК-10 ИД-1 ОПК-10 ИД-2 ОПК-2.2 ИД-1 ОПК-2.2 ИД-2 ОПК-2.3 ИД-3 ОПК-2.3 ИД-4 ОПК-2.4 ИД-3 ОПК-2.4 ИД-4	Самостоятельное выполнение заданий по заданным темам.	Конспект. Письменный отчет	7.85	0.25	8.1
Итого за 7 семестр			34.75	1.25	36
8 семестр					
ОПК-10 ИД-1 ОПК-10 ИД-2 ОПК-2.2 ИД-1 ОПК-2.2 ИД-2 ОПК-2.3 ИД-3 ОПК-2.3 ИД-4 ОПК-2.4 ИД-3 ОПК-2.4 ИД-4	Подготовка к экзамену	Вопросы к экзамену	1.55	0.25	1.8
ОПК-10 ИД-1 ОПК-10 ИД-2 ОПК-2.2 ИД-1 ОПК-2.2 ИД-2 ОПК-2.3 ИД-3 ОПК-2.3 ИД-4 ОПК-2.4 ИД-3 ОПК-2.4 ИД-4	Самостоятельное изучение литературы	Конспект	3.1	0.5	3.6
ОПК-10 ИД-1 ОПК-10 ИД-2 ОПК-2.2 ИД-1 ОПК-2.2 ИД-2 ОПК-2.3 ИД-3 ОПК-2.3 ИД-4 ОПК-2.4 ИД-3 ОПК-2.4 ИД-4	Подготовка к лабораторной работе	Собеседование	1.55	0.25	1.8
ОПК-10 ИД-1 ОПК-10 ИД-2 ОПК-2.2 ИД-1 ОПК-2.2 ИД-2 ОПК-2.3 ИД-3 ОПК-2.3 ИД-4 ОПК-2.4 ИД-3 ОПК-2.4 ИД-4	Подготовка к лекции	Конспект	1.55	0.25	1.8
Итого за 8 семестр			46.75	1.25	48
Итого			81.5	2.5	84

3. Порядок выполнения самостоятельной работы

3.1 Методические рекомендации по изучению теоретического материала

Комплексное изучение предлагаемой студентам учебной дисциплины «Комплексная система защиты информации на предприятии» предполагает овладение материалами лекций, учебников, программы, творческую работу студентов в ходе проведения лабораторных работ, а также систематическое выполнение заданий для самостоятельной работы.

В ходе лекций раскрываются основные вопросы в рамках рассматриваемых тем, делаются акценты на наиболее сложные и интересные положения изучаемого материала, которые должны быть приняты студентами во внимание. Материалы лекций являются основой для подготовки студентов к лабораторным занятиям.

Работа с конспектом лекций

Просмотрите конспект сразу после занятий. Отметьте материал конспекта лекций, который вызывает затруднения для понимания. Попробуйте найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь на текущей консультации или на ближайшей лекции за помощью к преподавателю.

Каждую неделю отводите время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам и тестам.

Выполнение лабораторных работ по дисциплине «Комплексная система защиты информации на предприятии»

На первом занятии получите у преподавателя задания по курсу, планы подготовки к лабораторным работам. Обзаведитесь всем необходимым методическим обеспечением.

Перед лабораторными работами изучите теорию вопроса, предполагаемого к исследованию, ознакомьтесь с опытом других исследователей в этом направлении.

Целью лабораторных работ является:

- ☐ закрепление методов приложения теории к решению практических задач анализа и синтеза психологического знания;
- ☐ проверка уровня понимания студентами вопросов, рассмотренных на лекциях и по учебной литературе, степени и качества усвоения материала;
- ☐ обучение навыкам освоения методики эксперимента и работы с нормативно-справочной литературой;
- ☐ восполнение пробелов в пройденной теоретической части курса и оказание помощи в его усвоении.

3.2 Методические рекомендации по конспектированию первоисточников

Изучение и анализ литературных источников является обязательным видом самостоятельной работы студентов. Изучение литературы по избранной теме имеет своей задачей проследить характер постановки и решения определенной проблемы различными авторами, аргументацию их выводов и обобщений, провести анализ и систематизировать полученный материал на основе собственного осмысления с целью выяснения современного состояния вопроса.

Проработка отобранного материала обязательно должна идти с одновременным ведением записей прочитанного и своих замечаний. Запись может иметь как форму конспекта, так и выписок, а также картотеку положений, тезисов, идей, методик, что в дальнейшем облегчит классификацию и систематизацию полученного материала. Такого рода записи являются лучшим способом накопления и первичной обработки материал, одной из обязательных форм организации умственного труда.

Планом удобно пользоваться при подготовке к устному выступлению по выбранной теме. Каждый пункт плана должен раскрывать одну из сторон избранной темы, а весь план должен охватывать ее целиком.

Тезисы предполагают сжатое изложение основных положений текста в форме утверждения или отрицания. Они являются более совершенной формой записей и представляют основу для дискуссии. К тому же их легко запомнить.

Конспектирование – процесс мысленной переработки и письменной фиксации информации, в виде краткого изложения основного содержания, смысла какого-либо текста.

Результат конспектирования – запись, позволяющая конспектирующему немедленно или через некоторый срок с нужной полнотой восстановить полученную информацию. Конспект в переводе с латыни означает «обзор». По существу его и составлять надо как обзор, содержащий основные мысли текста без подробностей и второстепенных деталей. Конспект носит индивидуализированный характер: он рассчитан на самого автора и поэтому может оказаться малопонятным для других.

Для того чтобы осуществлять этот вид работы, в каждом конкретном случае необходимо грамотно решить следующие задачи:

1. Сориентироваться в общей композиции текста (уметь определить вступление, основную часть, заключение).
2. Увидеть логико-смысловую канву сообщения, понять систему изложения автором информации в целом, а также ход развития каждой отдельной мысли.
3. Выявить «ключевые» мысли, т. е. основные смысловые вехи, на которые «нанизано» все содержание текста.
4. Определить детализирующую информацию.
5. Лаконично сформулировать основную информацию, не перенося на письмо все целиком и дословно.

Во всяком научном тексте содержится информация 2-х видов: основная и вспомогательная. Основной является информация, имеющая наиболее существенное значение для раскрытия содержания темы или вопроса. К ней относятся: определения научных понятий, формулировки законов, теоретических принципов и т. д. Назначение вспомогательной информации – помочь читателю лучше усвоить предлагаемый материал. К этому типу информации относятся разного рода комментарии. Основную – записываем как можно полнее, вспомогательную, как правило, опускаем. Содержание конспектирования составляет переработка основной информации в целях ее обобщения и сокращения. Обобщить – значит представить ее в более общей, схематической форме, в виде тезисов, выводов, отдельных заголовков, изложения основных результатов и т. п. Читая, мы интуитивно используем некоторые слова и фразы в качестве опорных. Такие опорные слова и фразы называются ключевыми. Ключевые слова и фразы несут основную смысловую и эмоциональную нагрузку содержания текста.

Выбор ключевых слов – это первый этап смыслового свертывания, смыслового сжатия материала.

Важными требованиями к конспекту являются наглядность и обозримость записей и такое их расположение, которое давало бы возможность уяснить логические связи и иерархию понятий.

По форме конспекты подразделяются на формализованные и графические.

1. Формализованные (все записи вносятся в заранее подготовленные таблицы).

Это удобно, во-первых, при конспектировании материалов, когда перечень характеристик описываемых предметов или явлений более или менее постоянен, во-вторых, при подготовке единого конспекта по нескольким источникам. Особенно если есть необходимость сравнения отдельных данных. Разновидностью формализованного конспекта является запись, составленная в форме ответов на заранее подготовленные вопросы, обеспечивающие исчерпывающие характеристики однотипных предметов или явлений.

2. Графические (элементы конспектируемой работы располагаются в таком виде, при котором видна иерархия понятий и взаимосвязь между ними).

По каждой работе может быть не один, а несколько графических конспектов, отображающих книгу в целом и отдельные ее части. Ведение графического конспекта – наиболее совершенный способ изображения внутренней структуры книги, а сам этот процесс помогает усвоению ее содержания.

Можно выделить следующие основные **типы конспектов: плановый, текстуальный, сводный, тематический.**

Плановый – легко получить с помощью предварительно сделанного плана произведения, каждому вопросу плана отвечает определенная часть конспекта:

а) вопросно-ответный (на пункты плана, выраженные в вопросительной форме, конспект дает точные ответы);

б) схематичный плановый конспект (отражает логическую структуру и взаимосвязь отдельных положений).

Текстуальный – это конспект, созданный в основном из цитат.

Сводный конспект – сочетает выписки, цитаты, иногда тезисы; часть его текста может быть снабжена планом.

Тематический – дает более или менее исчерпывающий ответ (в зависимости из числа привлеченных источников и другого материала, например, своих же записей) на поставленный вопрос – тему: обзорный; хронологический.

Роль конспекта – чисто учебная: он помогает зафиксировать основные понятия и положения первичного текста и в нужный момент их воспроизвести, например, при написании реферата или подготовке к экзамену. **Способы конспектирования.**

- **Тезисы** – это кратко сформулированные основные мысли, положения изучаемого материала. Тезисы лаконично выражают суть читаемого, дают возможность раскрыть содержание. Приступая к освоению записи в виде тезисов, полезно в самом тексте отмечать места, наиболее четко формулирующие основную мысль, которую автор доказывает (если, конечно, это не библиотечная книга). Часто такой отбор облегчается шрифтовым выделением, сделанным в самом тексте.

- **Линейно-последовательная запись текста.** При конспектировании линейно – последовательным способом целесообразно использование плакатно-оформительских средств, которые включают в себя следующие:

- сдвиг текста конспекта по горизонтали, по вертикали;
- выделение жирным (или другим) шрифтом особо значимых слов;
- использование различных цветов;
- подчеркивание;
- заключение в рамку главной информации.

- **Способ «вопросов – ответов».** Он заключается в том, что, поделив страницу тетради пополам вертикальной чертой, конспектирующий в левой части страницы самостоятельно формулирует вопросы или проблемы, затронутые в данном тексте, а в правой части дает ответы на них.

Одна из модификаций способа «вопросов – ответов» - таблица, где место вопроса занимает формулировка проблемы, поднятой автором (лектором), а место ответа – решение данной проблемы. Иногда в таблице могут появиться и дополнительные графы: например, «мое мнение» и т. п.

- **Схема с фрагментами** – способ конспектирования, позволяющий ярче выявить структуру текста, - при этом фрагменты текста (опорные слова, словосочетания, пояснения всякого рода) в сочетании с графикой помогают созданию рационально - лаконичного конспекта.

- **Простая схема** – способ конспектирования, близкий к схеме с фрагментами, объяснений к которой конспектирующий не пишет, но должен уметь давать их устно.

Этот способ требует высокой квалификации конспектирующего. В противном случае такой конспект нельзя будет использовать.

- **Параллельный способ** конспектирования. Конспект оформляется на двух листах параллельно или один лист делится вертикальной чертой пополам и записи делаются в правой и в левой части листа.

Однако лучше использовать разные способы конспектирования для записи одного и того же материала.

Комбинированный конспект – вершина овладения рациональным конспектированием. При этом умело используются все перечисленные способы, сочетая их в одном конспекте (один из видов конспекта свободно перетекает в другой в зависимости от конспектируемого текста, от желания и умения конспектирующего). Именно при комбинированном конспекте более всего проявляется уровень подготовки и индивидуальность студента. **Принципы составления конспекта прочитанного.**

1. Записать все выходные данные источника: автор, название, год и место издания. Если текст взят из периодического издания (газеты или журнала), то записать его название, год, месяц, номер, число, место издания.

2. Выделить поля слева или справа, можно с обеих сторон. Слева на полях отмечаются страницы оригинала, структурные разделы статьи или книги (названия параграфов, подзаголовки и т. п.), формулируются основные проблемы. Справа – способы фиксации прочитанной информации.

Один из видов чтения – углубленное – предполагает глубокое усвоение прочитанного и часто сохранение информации в целях последующего обращения к ней.

Эффективность такого чтения повышается, если прочитанное зафиксировано не только в памяти, но и на бумаге. Психологи утверждают, что записанное лучше и полнее усваивается, прочнее откладывается в памяти. Установлено, что если прочитать 1000 слов и затем записать 50, подытоживающих прочитанное, то коэффициент усвоения будет выше, чем, если прочитать 10000 слов, не записав ни одного. Кроме того, при записи прочитанного формируется навык свертывания информации. И, наконец, чередование чтения и записывания уменьшает усталость, повышает работоспособность и производительность умственного труда.

1. Резюмирование.

Резюме – краткий итог прочитанного, содержащий его оценку. Резюме характеризует основные выводы книги, главные итоги.

Выбор языковых средств для построения резюме-выводов подчинен основной задаче свертывания информации: минимум языковых средств – максимум информации. Это обычно одно – три четких, кратких, выразительных предложения, раскрывающих, по мнению автора, самую суть описываемого объекта.

2. Аннотация.

Аннотация – краткая обобщенная характеристика печатной работы (книги, статьи), включающая иногда и его оценку. Это наикратчайшее изложение содержания первичного документа, дающее общее представление о теме.

Основное ее назначение – дать некоторое представление о книге (статье, научной работе) с тем, чтобы рекомендовать ее определенному кругу читателей или воспользоваться своими записями при выполнении работы исследовательского, реферативного характера. Поэтому аннотации не требуются изложения содержания произведения, в ней лишь перечисляются вопросы, которые освещены в первоисточнике (содержание этих вопросов не раскрывается). Аннотация отвечает на вопрос: «О чем говорится в первичном тексте?», дает представление только о главной теме и перечне вопросов, затрагиваемых в тексте первоисточника.

Текст аннотации не стандартизирован. В научной литературе можно встретить различные требования к составлению аннотаций. Например, текст справочной аннотации может включать следующие сведения:

- тип и название аннотируемого документа (монография, диссертация, сборник, статья и т. п.)
- задачи, поставленные автором аннотируемого документа
- метод, которым пользовался автор (эксперимент, сравнительный анализ, компиляция других источников)
- принадлежность автора к определенной научной школе или направлению
- структуру аннотируемого документа
- предмет и тему произведения, основные положения и выводы автора
- характеристику вспомогательных иллюстративных материалов, дополнений, приложений, справочного аппарата, включая указатели и библиографию.

4.1 Вопросы для собеседования по лабораторным работам

Вопросы для проверки уровня обученности

- 1) Предмет и задачи комплексных систем защиты информации.
- 2) Информация и ее свойства как предмет защиты.
- 3) Методы определения количества информации.
- 4) Сущность и задачи построения комплекса систем защиты информации на предприятии.
- 5) Факторы, влияющие на защиту информации.
- 6) Определение и нормативное закрепление состава защищаемой информации.
- 7) Системный подход к защите информации.
- 8) Этапы по выявлению состава защищаемой информации.
- 9) Определение объектов защиты информации.
- 10) Системный подход к защите информации.
- 11) Моделирование комплекса систем защиты информации.
- 12) Методы неформального моделирования.
- 13) Концептуальная модель защиты информации.
- 14) Анализ и оценка угроз безопасности информации: выявление и оценка источников, воздействия на информацию.
- 15) Определение потенциальных каналов и методов несанкционированного доступа к информации.
- 16) Методика выявления каналов несанкционированного доступа к информации.
- 17) Методы и модели оценки уязвимости информации.
- 18) Виды обеспечения КСЗИ. Общая характеристика средств ЗИ.
- 19) Виды обеспечения КСЗИ. Организационное обеспечение процесса ЗИ.
- 20) Принципы организации и этапы разработки КСЗИ.
- 21) Виды обеспечения КСЗИ. Инженерно-техническое обеспечение ЗИ.
- 22) Особенности организационно-правовых методов защиты информации в России.
- 23) Защита информации от случайных угроз.
- 24) Защита информации от электромагнитных излучений и наводок.

25) Виды обеспечения КСЗИ. Математическое обеспечение процесса ЗИ.

26) Методы подбора технических средств ЗИ. Методы многокритериальных задач

27) Управление КСЗИ. Особенности управления КСЗИ

28) Технологическое и организационное построение КСЗИ.

Задачи для проверки умений и навыков

Повышенный уровень:

1) Опишите методику составления Перечня сведений, составляющих коммерческую тайну предприятия. Укажите функции должностных лиц, объединений и основных структурных подразделений (в произвольной форме с явным выделением этапов методики).

2) Разработайте Перечень сведений, составляющих коммерческую тайну предприятия согласно выбранному номеру варианта. Результаты представьте в виде таблицы.

3) Средства производства предприятия как объект защиты.

4) Средства вычислительной техники как объект защиты.

5) Определить возможные каналы утечки информации для защищаемого объекта.

6) Результаты анализа занести в таблицу. Указать не менее 10 технических каналов утечки.

7) Графически изобразите на плане предприятия выявленные технические каналы утечки информации.

8) Обоснование выбранных вариантов системы в докладной записке или в проекте для руководства организации.

9) Доработка вариантов или проекта с учетом замечаний руководства.

Вопросы для проверки уровня обученности

- 1) Инженерно-техническая защита охраняемого объекта.
- 2) Разработка модели КСЗИ. Модель потенциального нарушителя.
- 3) Разработка модели КСЗИ. Функциональная модель КСЗИ.
- 4) Обеспечение функционирования КСЗИ. Нормативно-методические документы, обеспечивающие функционирование СЗИ.
- 5) Обеспечение функционирования КСЗИ. Подбор и обучение персонала.
- 6) Аналитические и имитационные модели КСЗИ.
- 7) Структура управления системой защиты информации предприятия.
- 8) Управление КСЗИ в условиях чрезвычайных ситуаций.
- 9) Сущность и содержание контроля функционирования КСЗИ.
- 10) Разработка и внедрение политики информационной безопасности.
- 11) Кадровое обеспечение КСЗИ.
- 12) Состав методов и моделей оценки эффективности КСЗИ.

Задачи для проверки умений и навыков

- 1) Представить состав основных функций и организационных элементов КСЗИ.
- 2) Объяснить, как содержательно взаимосвязаны функциональная и организационная структуры КСЗИ.
- 3) Построить и графически представить функциональную и организационную модели системы защиты информации объекта, описание которого приведено выше.
- 4) Проанализировать угрозы, начиная с угроз, имеющих максимальное значение, далее - с меньшей угрозой и так далее до тех пор, пока не будут исчерпаны выделенные ресурсы.
- 5) Принять решение по инженерно-технической защите охраняемого объекта, результаты оформить таблицей.
- 6) Разработать Примерный перечень исходных данных необходимых для анализа состояния дел по вопросам обеспечения информационной безопасности, разработки предложений по совершенствованию безопасности, разработки предложений

по совершенствованию системы защиты и организационно-распорядительных документов.

7) Разработать Соглашение (обязательство) о соблюдении требований обращения с защищаемой информацией.

8) Разработать Инструкцию по организации парольной защиты автоматизированной системы.

9) Общие сведения об организации (название, сфера деятельности, общая численность сотрудников);

10) Скриншоты работы с программой "Оценка СЗИ" (профиль защиты: количественный, качественный, система в целом)

На основе полученных данных сделать выводы о состоянии КСЗИ и определить её сильные и слабые места, выбрать направления по дальнейшему совершенствованию КСЗИ.

4.3 Комплект разноуровневых задач и заданий

Базовый уровень

7 семестр:

Тема 1: Базовые понятия дисциплины

4. Источники и литература по курсу. Методика самостоятельной работы студентов по изучению курса.

5. Знания и умения студентов, которые должны быть получены в результате изучения курса. Основные термины и определения в области КСЗИ.

Тема 2: Сущность и задачи комплексной системы защиты информации

4. КСЗИ как средство выражения концептуальных основ защиты информации.

5. Методология защиты информации как теоретический базис построения КСЗИ.

Тема 3: Принципы организации и этапы разработки комплексной системы защиты информации

4. Принципы организации КСЗИ.
5. Основные требования, предъявляемые к КСЗИ.
6. Содержательная характеристика этапов разработки КСЗИ.

Тема 4: Определение и нормативное закрепление состава защищаемой информации

4. Классификация информации по видам тайны и степеням конфиденциальности.
5. Нормативное закрепление состава защищаемой информации; структура перечней сведений, относимых к различным видам тайны.
6. Порядок внедрения перечней, внесения в них изменений и дополнений.

Тема 5: Определение объектов защиты

4. Хранилища носителей информации как объект защиты.
5. Особенности помещений для работы с защищаемой информацией как объектов защиты.
6. Состав технических средств обработки, передачи, транспортировки и защиты информации, являющихся объектами защиты.
7. Состав средств обеспечения функционирования предприятия, подлежащих защите.
8. Факторы, определяющие необходимость защиты периметра и здания предприятия.
9. Специфика персонала предприятия как объекта защиты.

Тема 6: Выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию

4. Оценка ущерба от потенциального дестабилизирующего воздействия на информацию.

Тема 7: Определение потенциальных каналов и методов несанкционированного доступа к информации

4. Оценка степени опасности применения различных методов.
5. Анализ потенциальных последствий реализации несанкционированного доступа.

Тема 8: Определение условий функционирования комплексной системы защиты информации

3. Обеспечение безопасности всей совокупности подлежащей защите информации во всех компонентах ее сбора, хранения, передачи и использования, а также во все время и при всех режимах функционирования систем обработки информации.

Тема 9: Разработка модели комплексной системы защиты информации

4. Выбор структуры комплексной системы защиты информации, ее зависимость от объектов защиты, характера и условий функционирования предприятия.
5. Функциональная модель комплексной системы защиты информации.
6. Организационная модель комплексной системы защиты информации.
7. Информационная модель комплексной системы защиты информации.

8 семестр:

Тема 10: Технологическое и организационное построение комплексной системы защиты информации

4. Предпроектное обследование, технический проект, рабочий проект.
5. Аprobация и ввод в эксплуатацию.

Тема 11: Кадровое обеспечение функционирования комплексной системы защиты информации

4. Подбор и обучение персонала.

Тема 12: Материально-техническое и нормативно-методическое обеспечение комплексной системы защиты информации

4. Перечень вопросов, требующих документационного закрепления.
5. Состав нормативно-методических документов по обеспечению функционирования комплексной системы защиты информации, их назначение, структура и содержание.
6. Порядок разработки и внедрения документов

Тема 13: Назначение, структура и содержание управления комплексной системой защиты информации

4. Основные стили управления. Структура и содержание общей технологии управления комплексной системой защиты информации.

Тема 14: Принципы и методы планирования функционирования комплексной системы защиты информации

4. Структура и общее содержание планов организации и функционирования комплексной системы защиты информации.
5. Методы сбора, обработки и изучения информации, необходимой для планирования.
6. Организация выполнения планов.

Тема 15: Сущность и содержание контроля функционирования комплексной системы защиты информации

4. Анализ и использование результатов проведения контрольных мероприятий.

Тема 16: Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций

4. Подготовка мероприятий на случай возникновения чрезвычайных ситуаций.

Тема 17: Оценка эффективности комплексной системы защиты информации

4. Содержание и особенности экспертной оценки эффективности защиты: выбор системы измерений (вербальные и вербально-числовые шкалы), организация процедуры экспертного оценивания (подбор экспертов, составление вопросников, обработка результатов).

5. Сравнительный анализ подходов.

Тема 18: Методы и модели оценки эффективности комплексной системы защиты информации

4. Метод оценки уровня безопасности и аналитические модели определения базовых и обобщенных показателей уязвимости.

5. Метод построения "розеток" (диаграмм) безопасности.

6. Метод анализа риска.

7. Метод оценки на основе структурных вопросников.

8. Области применения и анализ приемлемости различных методов и моделей для решения задачи оценки эффективности КСЗИ

3.4 Методические указания для подготовки к экзамену

Вопросы к экзамену

Вопросы для проверки уровня обученности

- 29) Предмет и задачи комплексных систем защиты информации.
- 30) Информация и ее свойства как предмет защиты.
- 31) Методы определения количества информации.
- 32) Сущность и задачи построения комплекса систем защиты информации на предприятии.
- 33) Факторы, влияющие на защиту информации.
- 34) Определение и нормативное закрепление состава защищаемой информации.
- 35) Системный подход к защите информации.
- 36) Этапы по выявлению состава защищаемой информации.
- 37) Определение объектов защиты информации.
- 38) Системный подход к защите информации.

- 39) Моделирование комплекса систем защиты информации.
- 40) Методы неформального моделирования.
- 41) Концептуальная модель защиты информации.
- 42) Анализ и оценка угроз безопасности информации: выявление и оценка источников, воздействия на информацию.
- 43) Определение потенциальных каналов и методов несанкционированного доступа к информации.
- 44) Методика выявления каналов несанкционированного доступа к информации.
- 45) Методы и модели оценки уязвимости информации.
- 46) Виды обеспечения КСЗИ. Общая характеристика средств ЗИ.
- 47) Виды обеспечения КСЗИ. Организационное обеспечение процесса ЗИ.
- 48) Принципы организации и этапы разработки КСЗИ.
- 49) Виды обеспечения КСЗИ. Инженерно-техническое обеспечение ЗИ.
- 50) Особенности организационно-правовых методов защиты информации в России.
- 51) Защита информации от случайных угроз.
- 52) Защита информации от электромагнитных излучений и наводок.
- 53) Виды обеспечения КСЗИ. Математическое обеспечение процесса ЗИ.
- 54) Методы подбора технических средств ЗИ. Методы многокритериальных задач
- 55) Управление КСЗИ. Особенности управления КСЗИ
- 56) Технологическое и организационное построение КСЗИ.

Задачи для проверки умений и навыков

Повышенный уровень:

- 10) Опишите методику составления Перечня сведений, составляющих коммерческую тайну предприятия. Укажите функции должностных лиц,

объединений и основных структурных подразделений (в произвольной форме с явным выделением этапов методики).

11) Разработайте Перечень сведений, составляющих коммерческую тайну предприятия согласно выбранному номеру варианта. Результаты представьте в виде таблицы.

12) Средства производства предприятия как объект защиты.

13) Средства вычислительной техники как объект защиты.

14) Определить возможные каналы утечки информации для защищаемого объекта.

15) Результаты анализа занести в таблицу. Указать не менее 10 технических каналов утечки.

16) Графически изобразите на плане предприятия выявленные технические каналы утечки информации.

17) Обоснование выбранных вариантов системы в докладной записке или в проекте для руководства организации.

18) Доработка вариантов или проекта с учетом замечаний руководства.

Вопросы для проверки уровня обученности

13) Инженерно-техническая защита охраняемого объекта.

14) Разработка модели КСЗИ. Модель потенциального нарушителя.

15) Разработка модели КСЗИ. Функциональная модель КСЗИ.

16) Обеспечение функционирования КСЗИ. Нормативно-методические документы, обеспечивающие функционирование СЗИ.

17) Обеспечение функционирования КСЗИ. Подбор и обучение персонала.

18) Аналитические и имитационные модели КСЗИ.

19) Структура управления системой защиты информации предприятия.

20) Управление КСЗИ в условиях чрезвычайных ситуаций.

21) Сущность и содержание контроля функционирования КСЗИ.

22) Разработка и внедрение политики информационной безопасности.

23) Кадровое обеспечение КСЗИ.

24) Состав методов и моделей оценки эффективности КСЗИ.

Задачи для проверки умений и навыков

11) Представить состав основных функций и организационных элементов КСЗИ.

12) Объяснить, как содержательно взаимосвязаны функциональная и организационная структуры КСЗИ.

13) Построить и графически представить функциональную и организационную модели системы защиты информации объекта, описание которого приведено выше.

14) Проанализировать угрозы, начиная с угроз, имеющих максимальное значение, далее - с меньшей угрозой и так далее до тех пор, пока не будут исчерпаны выделенные ресурсы.

15) Принять решение по инженерно-технической защите охраняемого объекта, результаты оформить таблицей.

16) Разработать Примерный перечень исходных данных необходимых для анализа состояния дел по вопросам обеспечения информационной безопасности, разработки предложений по совершенствованию безопасности, разработки предложений по совершенствованию системы защиты и организационно-распорядительных документов.

17) Разработать Соглашение (обязательство) о соблюдении требований обращения с защищаемой информацией.

18) Разработать Инструкцию по организации парольной защиты автоматизированной системы.

19) Общие сведения об организации (название, сфера деятельности, общая численность сотрудников);

20) Скриншоты работы с программой "Оценка СЗИ" (профиль защиты: количественный, качественный, система в целом)

На основе полученных данных сделать выводы о состоянии КСЗИ и определить её сильные и слабые места, выбрать направления по дальнейшему совершенствованию КСЗИ.

4.3 Комплект разноуровневых задач и заданий

Базовый уровень

7 семестр:

Тема 1: Базовые понятия дисциплины

4. Источники и литература по курсу. Методика самостоятельной работы студентов по изучению курса.

5. Знания и умения студентов, которые должны быть получены в результате изучения курса. Основные термины и определения в области КСЗИ.

Тема 2: Сущность и задачи комплексной системы защиты информации

4. КСЗИ как средство выражения концептуальных основ защиты информации.

5. Методология защиты информации как теоретический базис построения КСЗИ.

Тема 3: Принципы организации и этапы разработки комплексной системы защиты информации

4. Принципы организации КСЗИ.

5. Основные требования, предъявляемые к КСЗИ.

6. Содержательная характеристика этапов разработки КСЗИ.

Тема 4: Определение и нормативное закрепление состава защищаемой информации

4. Классификация информации по видам тайны и степеням конфиденциальности.

5. Нормативное закрепление состава защищаемой информации; структура перечней сведений, относимых к различным видам тайны.

6. Порядок внедрения перечней, внесения в них изменений и дополнений.

Тема 5: Определение объектов защиты

4. Хранилища носителей информации как объект защиты.

5. Особенности помещений для работы с защищаемой информацией как объектов защиты.

6. Состав технических средств обработки, передачи, транспортировки и защиты информации, являющихся объектами защиты.

7. Состав средств обеспечения функционирования предприятия, подлежащих защите.

8. Факторы, определяющие необходимость защиты периметра и здания предприятия.

9. Специфика персонала предприятия как объекта защиты.

Тема 6: Выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию

4. Оценка ущерба от потенциального дестабилизирующего воздействия на информацию.

Тема 7: Определение потенциальных каналов и методов несанкционированного доступа к информации

4. Оценка степени опасности применения различных методов.

5. Анализ потенциальных последствий реализации несанкционированного доступа.

Тема 8: Определение условий функционирования комплексной системы защиты информации

3. Обеспечение безопасности всей совокупности подлежащей защите информации во всех компонентах ее сбора, хранения, передачи и использования, а также во все время и при всех режимах функционирования систем обработки информации.

Тема 9: Разработка модели комплексной системы защиты информации

4. Выбор структуры комплексной системы защиты информации, ее зависимость от объектов защиты, характера и условий функционирования предприятия.
5. Функциональная модель комплексной системы защиты информации.

6. Организационная модель комплексной системы защиты информации.

7. Информационная модель комплексной системы защиты информации.

8 семестр:

Тема 10: Технологическое и организационное построение комплексной системы защиты информации

4. Предпроектное обследование, технический проект, рабочий проект.
5. Аprobация и ввод в эксплуатацию.

Тема 11: Кадровое обеспечение функционирования комплексной системы защиты информации

4. Подбор и обучение персонала.

Тема 12: Материально-техническое и нормативно-методическое обеспечение комплексной системы защиты информации

4. Перечень вопросов, требующих документационного закрепления.
5. Состав нормативно-методических документов по обеспечению функционирования комплексной системы защиты информации, их назначение, структура и содержание.
6. Порядок разработки и внедрения документов

Тема 13: Назначение, структура и содержание управления комплексной системой защиты информации

4. Основные стили управления. Структура и содержание общей технологии управления комплексной системой защиты информации.

Тема 14: Принципы и методы планирования функционирования комплексной системы защиты информации

4. Структура и общее содержание планов организации и функционирования комплексной системы защиты информации.

5. Методы сбора, обработки и изучения информации, необходимой для планирования.

6. Организация выполнения планов.

Тема 15: Сущность и содержание контроля функционирования комплексной системы защиты информации

4. Анализ и использование результатов проведения контрольных мероприятий.

Тема 16: Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций

4. Подготовка мероприятий на случай возникновения чрезвычайных ситуаций.

Тема 17: Оценка эффективности комплексной системы защиты информации

4. Содержание и особенности экспертной оценки эффективности защиты: выбор системы измерений (вербальные и вербально-числовые шкалы), организация процедуры экспертного оценивания (подбор экспертов, составление вопросников, обработка результатов).

5. Сравнительный анализ подходов.

Тема 18: Методы и модели оценки эффективности комплексной системы защиты информации

4. Метод оценки уровня безопасности и аналитические модели определения базовых и обобщенных показателей уязвимости.

5. Метод построения "розеток" (диаграмм) безопасности.

6. Метод анализа риска.
7. Метод оценки на основе структурных вопросников.
8. Области применения и анализ приемлемости различных методов и моделей для решения задачи оценки эффективности КСЗИ

Список рекомендуемой литературы

Основная литература

1. Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии. – М. Издательский дом "Академия", 2009. – 416 с.
2. Гришина Н.В. Комплексная система защиты информации на предприятии. – М.: Форум, 2009. – 240 с.
3. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. – М.: Инфра-М, Форум, 2010. – 592 с.

Дополнительная литература

1. Северин В.А. Комплексная защита информации на предприятии. – Городец, 2008. – 368 с.
2. Гришина Н.В. Организация комплексной системы защиты информации. – М.: Гелиос АРВ, 2007. – 256 с.
3. Завгородний В.И. Комплексная защита информации в компьютерных системах. – М.: Логос, 2001. – 264с.
4. Шевцов В.А., Куприянов А.И., Сахаров А.В. Основы защиты информации. – М. Издательский дом "Академия", 2008. – 256 с.
5. Конеев И.Р. Информационная безопасность предприятий. - СПб.: БХВПетербург, 2003.- 752 с.
6. Ярочкин В.И. Информационная безопасность. – М.: Академический Проект: Фонд "Мир", 2003. – 640 с.

Интернет-ресурсы

1. Официальный сайт Федеральной службы по техническому и экспортному контролю. – www.fstec.ru;
2. Официальный сайт Федеральной служба безопасности Российской Федерации. – www.fsb.ru.
3. Защита информации, управление информационной безопасностью и рисками.
www.iso27000.ru

5.1.5. Программное обеспечение

- программное обеспечение: Microsoft Office Excel или Open Office Calc, файловый менеджер Far, архиватор WinRAR, Adobe Acrobat Reader или FoxIT Reader.
- программы тестового контроля Iren.

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

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для обучающихся по организации и проведению курсовой работы
по дисциплине «Комплексная система защиты информации на
предприятии»

для студентов направления подготовки

10.03.01 «Информационная безопасность»

Направленность (профиль):

«Организация и технологии защиты информации (по отрасли или в
сфере профессиональной деятельности)»

Ставрополь

2026

Содержание 1 Общие требования к выполнению курсовой работы **Ошибка!**
Закладка не определена.

1.1 Цели и задачи курсовой работы	4
1.2 Тематика курсовых работ	5
1.3 Содержание и структура курсовых работ	6
2. Рекомендации по подготовке и оформлению курсовой работы	8
2.1 Изложение текста	11
2.2 Формулы	13
2.3 Иллюстрации и приложения	15
2.4 Таблицы	18
3 Организация выполнения и порядок руководства курсовыми работами	21
4. Защита курсовых работ	22
Приложение А	24
Приложение Б	27
Приложение В	31
Приложение Г	38
Приложение Д	38

1 Общие требования к выполнению курсовой работы

Курсовая работа – обязательный вид учебной работы, выполняется студентом в течение семестра.

Курсовая работ является самостоятельной исследовательской работой студента и представляет собой логически завершенное и оформленное научное исследование. Курсовая работа направлена на формирование у студента навыков научно-исследовательской работы, повышение уровня его профессиональной (теоретической и практической) подготовки, углубление знаний по учебной дисциплине, развитие интереса и навыков самостоятельной работы с научной и справочной литературой.

1.1 Цели и задачи курсовой работы

Выполнение курсовой работы имеет целью расширение знаний студентов, обучение методам теоретического анализа явлений и закономерностей науки, отработку навыков самостоятельного применения теоретических знаний к комплексному решению профессиональных задач, использования справочной литературы, методов математической обработки экспериментальных данных, компьютерных технологий.

Системой курсовых работ студент подготавливается к выполнению выпускной квалификационной работы.

В процессе выполнения курсовой работы студентом должны решаться следующие задачи:

- приобретение новых теоретических знаний в соответствии с темой работы и заданием руководителя;

- развитие умений систематизировать, обобщать и логично излагать концепции, альтернативные точки зрения исследуемых проблем;
- развитие учебно-исследовательских и методических умений, необходимых для построения системы научного анализа изучаемого аспекта; ○ совершенствование профессиональной подготовки.

1.2 Тематика курсовых работ

Одним из важных компонентов в системе постановки курсового проектирования (курсовой работы) является правильное определение тематики.

Тематика курсовых работ должна быть актуальной, отвечать учебным задачам данного предмета, а также потребностям науки и практики. Актуальность тематики курсовых работ - это, прежде всего, научность, современность и направленность к получению студентами навыков самостоятельной творческой работы.

Темы курсовых работ должны быть комплексными, т.е. содержать ряд взаимосвязанных между собой проблем и строиться на фактическом материале профильных предприятий и учреждений, а также на итогах учебной и производственной практики студентов, на научных работах членов кафедры, студенческих научных кружков и проблемных групп, с использованием новейших достижений отечественной и зарубежной науки, актуальных прикладных аспектов.

Темы курсовых работ утверждаются на заседании кафедры, ведущей дисциплины, по которым учебными планами предусмотрены курсовые работы. Выписка из протокола заседания кафедры передается в дирекцию института, где формируется распоряжение об утверждении тем курсовых работ. В течение 10 дней после выхода распоряжения об утверждении тем курсовых работ специалист по учебно-методической работе дирекции вносит названия тем в автоматизированную базу университета.

Основные содержательные и процессуальные аспекты, необходимые для выполнения работы, оформляются кафедрой в заданиях на курсовую работу (Приложение А). В заданиях необходимо четко сформулировать название темы работы и требования, определяющие его объем, содержание, а также исходные данные для выполнения количественных расчетов.

1.3 Содержание и структура курсовых работ

Курсовая работа (проект) должна содержать элементы новизны, наряду с фундаментальным аспектом должен быть проведен анализ современного состояния изучаемой проблемы, а также отражены региональные особенности.

Задание по курсовой работе необходимо индивидуализировать с учетом интересов и способностей студентов.

Курсовая работа (проект) должна состоять из:

- содержания;
- введения;
- теоретической части;
- эмпирической части;
- заключения;
- списка использованных источников; - приложения.

В отдельных случаях, в соответствии с тематикой работы, эмпирическая часть может отсутствовать.

Титульный лист оформляется в соответствии с Приложением Б.

Содержание включает названия разделов, подразделов работы с указанием страницы начала каждой части (Приложение В).

Во введении обосновывается актуальность выбранной темы исследования; отражаются объект, предмет, задачи, цели, методы, новизна, теоретическая и практическая значимость исследования.

Теоретическая часть должна содержать анализ состояния изучаемой проблемы на основе обзора научной, научно-информационной, справочной литературы. Представленный материал должен быть логически связан с целью исследования. В параграфах теоретической части необходимо отражать отдельные компоненты проблемы и завершать их выводами.

Эмпирическая (практическая, расчетно-графическая) часть (при наличии) включает описание системы экспериментального исследования, обоснование методов исследования, анализ результатов экспериментального исследования, схемы, графические и математические способы интерпретации полученных данных, выводы.

Заключение содержит выводы, подтверждающие или опровергающие первоначальные предположения (гипотезы), перспективы дальнейшего изучения проблемы, связь с практикой, анализ реализации целей и задач исследования.

Список использованных источников должен содержать перечень всех используемых автором нормативных документов, монографий, учебных и учебно-методических пособий, статей и интернет-источников (Приложение Г).

При ссылке в тексте номер источника из списка литературы заключается в квадратные скобки, например, [1], [1, 3-4] или [1-2].

Приложение содержит весь фактический материал экспериментальных исследований (анкеты, опросники, схемы, чертежи, расчетные материалы, карты, рисунки, ответы респондентов и т.д.).

2. Рекомендации по подготовке и оформлению курсовой работы

Курсовые работы (проекты) рекомендуется представлять в объеме 30-40 страниц. Текст работы должен быть напечатан через 1,5 интервала на одной стороне стандартного листа белой бумаги (А - 4).

Текст курсовой работы выполняют с использованием компьютера на одной стороне листа белой бумаги, формата А4, шрифт - Times New Roman 14-го размера, межстрочный интервал - 1,5. Номер страницы проставляют в правом нижнем углу листа. Страницы текстового материала следует нумеровать арабскими цифрами, соблюдая сквозную нумерацию по всему документу. Титульный лист текстового документа включают в общую нумерацию страниц. Номер страницы на титульном листе не проставляют. Расстояние от края бумаги до границ текста следует оставлять: в начале строк - 30 мм; в конце строк - 10 мм; от верхней или нижней строки текста до верхнего или нижнего края бумаги - 20 мм. Размер абзацного отступа должен быть одинаковым по всему тексту работы и равным 12,5 мм.

Разделы должны иметь порядковые номера в пределах всей курсовой работы, обозначенные арабскими цифрами. Подразделы должны иметь нумерацию в пределах каждого раздела. Номера подразделов состоят из номера раздела и подраздела, разделенных точкой. В конце номера подраздела точка не ставится. Нумерация пунктов должна состоять из номера раздела, подраздела и пункта, разделенных точкой.

Заголовок разделов, подразделов и пунктов следует печатать с абзацного отступа, с прописной буквы, без точки в конце, не подчеркивая. Переносы слов в заголовках не допускаются. Если заголовок состоит из двух предложений, их разделяют точкой.

Ниже каждого заголовка должна быть оставлена одна свободная строка, выше - не менее одной свободной строки. Оставляют свободные строки между разделами и подразделами.

Пример

1 Методы испытаний

1.1 Аппараты, материалы и реактивы 2 Подготовка к испытанию

2.1 Нумерация пунктов первого подраздела третьего раздела доку-

мента 3

3.2 Подготовка к испытанию

3.3 Нумерация пунктов второго подраздела третьего раздела доку-

мента

Если раздел или подраздел состоит из одного пункта, он также нумеруется. Если текст документа подразделяется только на пункты, они нумеруются порядковыми номерами в пределах документа.

Пункты, при необходимости, могут быть разбиты на подпункты, которые должны иметь порядковую нумерацию в пределах каждого пункта, например: 4.2.1; 4.2.1.1; 4.2.1.2; 4.2.2 и т. д. Между подпунктами и текстом интервалы не оставляются. Подпункты с тройной нумерацией (1.1.1...) и больше в содержание не выносятся.

Внутри пунктов или подпунктов могут быть приведены перечисления.

Перед каждым перечислением следует ставить дефис или, при необходимости ссылки в тексте документа на одно из перечислений, строчную букву, после которой ставится скобка.

Для дальнейшей детализации перечислений необходимо использовать цифры, после которых ставится скобка, а запись производится с абзацного отступа, как показано в примере.

Пример:

- _____

- _____
1) _____
2) _____
- _____

Каждый раздел курсовой работы следует начинать с нового листа (страницы).

В документе большого объема на первом (заглавном) листе помещают содержание, включающее номера и наименования разделов и подразделов с указанием номеров листов (страниц). Содержание включают в общее количество листов

данного документа. Слово "Содержание" записывают в виде заголовка (симметрично тексту) с прописной буквы. Наименования, включенные в содержание, записывают строчными буквами, начиная с прописной буквы.

9

Список использованных источников должен быть оформлен в соответствии с ГОСТом 7.1-2003 «Библиографическая запись. Библиографическое описание».

2.1 Изложение текста

Текст документа должен быть кратким, четким и не допускать различных толкований.

При изложении обязательных требований в тексте должны применяться слова "должен", "следует", "необходимо", "требуется, чтобы", "разрешается только", "не допускается", "запрещается", "не следует". При изложении других положений следует применять слова - "могут быть", "как правило", "при необходимости", "может быть", "в случае" и т.д.

При этом допускается использовать повествовательную форму изложения текста документа, например "применяют", "указывают" и т.п.

В тексте должны применяться научно-технические термины, обозначения и определения, установленные соответствующими стандартами, а при их отсутствии – общепринятые в научно-технической литературе.

В тексте не допускается:

- применять обороты разговорной речи, техницизмы, профессионализмы;
- применять для одного и того же понятия различные научно-технические термины, близкие по смыслу (синонимы), а также иностранные слова при наличии равнозначных слов и терминов на русском языке;
- сокращать обозначения единиц физических величин, если они употребляются без цифр, за исключением единиц физических величин в головках и боковиках таблиц, в расшифровках буквенных обозначений, входящих в формулы и рисунки; применять математический знак минус (-) перед отрицательными значениями величин (следует писать слово «минус»);
- применять без числовых значений математические знаки, например, $>$ (больше), $<$ (меньше), $=$ (равно), $\neq$ (не равно), а также знака № (номер), % (процент); применять индексы стандартов без регистрирующего номера; перечень допускаемых сокращений слов установлен в ГОСТ 2.316, ГОСТ 7.12; в тексте следует применять стандартизованные единицы физических величин, их наименование и обозначение, установленные в ГОСТ 8.417;
- если в тексте курсовой работы приводится диапазон числовых значений физической величины, то обозначение единицы физической величины указывается, после последнего числового значения диапазона.

Примеры: 1. От 1 до 5 мм.

2. От плюс 10 до минус 40° С.

Недопустимо отделять единицу физической величины от числового зна-

чения (переносить их на разные строки или страницы), кроме единиц физических величин, помещенных в таблицах, выполненных машинописным способом.

2.2 Формулы

Уравнения и формулы следует выделять из текста в отдельную строку. Выше и ниже каждой формулы или уравнения должно быть оставлено не менее одной свободной строки. Если уравнение не умещается в одну строку, то оно должно быть перенесено после знака равенства (=) или после знаков плюс (+), минус (-), умножения (х), деления (:), или других математических знаков, причем знак в начале следующей строки повторяют. При переносе формулы на знаке, символизирующем операцию умножения, применяют знак «Х».

Пояснение значений символов и числовых коэффициентов следует приводить непосредственно под формулой в той же последовательности, в которой они даны в формуле.

Формулы в курсовой работе следует нумеровать порядковой нумерацией в пределах всей курсовой работы арабскими цифрами в круглых скобках в крайнем правом положении на строке.

Формулы, за исключением формул, помещаемых в приложениях, должны

нумероваться сквозной нумерацией арабскими цифрами, которые записывают на уровне формулы справа в круглых скобках. Одну формулу обозначают - (1).

Формулы, помещаемые в приложениях, должны нумероваться отдельной нумерацией арабскими цифрами в пределах каждого приложения с добавлением перед каждой цифрой обозначения приложения, например формула (B.1).

Допускается нумерация формул в пределах раздела. В этом случае номер формулы состоит из номера раздела и порядкового номера формулы, разделенных точкой, например (3.1).

После формулы помещают перечень всех принятых в формуле символов с расшифровкой их значений и указанием размерности (если в этом есть необходимость). Буквенные обозначения дают в той же последовательности, в которой они приведены в формуле. Первая строка пояснения должна начинаться со слова «где» без двоеточия после него.

$$PS \left(\mathbb{P} \left(F, Z, I \right) \right), \quad (1)$$

где F - рабочая память системы (называемая также базой данных), содержащая текущие данные (элементы рабочей памяти);

Z - база знаний, содержащая множество продукций (правил вида: "условие → действие");

I - интерпретатор (решатель), реализующий процедуры вывода. Формулы, следующие одна за другой и не разделенные текстом, разделяют запятой.

Формулы, помещаемые в приложениях, должны нумероваться отдельной нумерацией арабскими цифрами в пределах каждого приложения с добавлением перед каждой цифрой обозначения приложения, например формула (В. 1).

Ссылки в тексте на порядковые номера формул дают в скобках.

Пример -... в формуле (1).

2.3 Иллюстрации и приложения

Иллюстрации (чертежи, графики, схемы, компьютерные распечатки, диаграммы, фотоснимки) следует располагать в курсовой работе непосредственно после текста, в котором они упоминаются впервые, или на следующей странице.

Иллюстрации могут быть в компьютерном исполнении, в том числе и цветные.

На все иллюстрации должны быть даны ссылки в курсовой работе. Чертежи, графики, диаграммы, схемы, иллюстрации, помещаемые в курсовой работе, должны соответствовать требованиям государственных стандартов Единой системы конструкторской документации (ЕСКД).

Допускается выполнение чертежей, графиков, диаграмм, схем посредством использования компьютерной печати.

Фотоснимки размером меньше формата А4 должны быть наклеены на стандартные листы белой бумаги.

Иллюстрации, за исключением иллюстрации приложений, следует нумеровать арабскими цифрами сквозной нумерацией. Если рисунок один, то он обо-

значается «Рисунок 1». Слово «рисунок» и его наименование располагают посередине строки.

Иллюстрации каждого приложения обозначают отдельной нумерацией арабскими цифрами с добавлением перед цифрой обозначения приложения. Например - Рисунок А.3.

Допускается нумеровать иллюстрации в пределах раздела. В этом случае номер иллюстрации состоит из номера раздела и порядкового номера иллюстрации, разделенных точкой. Например Рисунок 1.1.

Выше и ниже каждой иллюстрации должно быть оставлено не менее одной свободной строки.

Пример: Цели и задачи



Рисунок 1 – Основные характеристики системы защиты

Иллюстрации, при необходимости, могут иметь наименование и пояснительные данные (подрисуночный текст).

Иллюстрации каждого приложения обозначают отдельной нумерацией арабскими цифрами с добавлением перед цифрой обозначения приложения.

Например, Рисунок А.3.

При ссылках на иллюстрации следует писать «... в соответствии с рисунком 2».

Материал, дополняющий текст документа, допускается помещать в при-

ложениях. Приложениями могут быть, например, графический материал, таблицы большого формата, расчеты, описания аппаратуры и приборов, описания алгоритмов и программ задач, решаемых на ЭВМ и т.д.

Приложение оформляют как продолжение данного документа на последующих его листах или выпускают в виде самостоятельного документа.

Каждое приложение следует начинать с новой страницы с указанием наверху посередине страницы слова "Приложение" и его обозначения, а под ним в скобках для обязательного приложения пишут слово "обязательное", а для информационного - "рекомендуемое" или "справочное".

Приложение должно иметь заголовок, который записывают симметрично относительно текста с прописной буквы отдельной строкой.

Приложения обозначают заглавными буквами русского алфавита, начиная с А, за исключением букв Ё, З, Й, О, Ч, Ь, Ы, Ъ. После слова "Приложение" следует буква, обозначающая его последовательность. Приложения, как правило, выполняют на листах формата А4. Допускается оформлять приложения на листах формата А3, А4 3, А4 4, А2 и А1 по ГОСТ 2.301.

Приложения должны иметь общую с остальной частью документа сквозную нумерацию страниц.

Пример:

Приложение А

(обязательное)

Все приложения должны быть перечислены в содержании документа (при наличии) с указанием их номеров и заголовков.

2.4 Таблицы

Таблицы применяют для лучшей наглядности и удобства сравнения показателей. Название таблицы, при его наличии, должно отражать ее содержание, быть точным, кратким. Слово "Таблица" указывают один раз слева над первой частью таблицы, над другими частями пишут слова "Продолжение таблицы" с указанием номера (обозначения) таблицы. При переносе части таблицы название помещают только над первой частью таблицы, нижнюю горизонтальную черту, ограничивающую таблицу, не проводят.

Таблицу следует располагать в курсовой работе непосредственно после текста, в котором она упоминается впервые, или на следующей странице, а при необходимости, в приложении к документу.

Допускается помещать таблицу вдоль длинной стороны листа документа. На все таблицы должны быть ссылки в отчете. При ссылке следует писать слово «таблица» с указанием ее номера.

Таблицу с большим количеством строк допускается переносить на другой лист (страницу).

При переносе части таблицы на другой лист (страницу) слово «Таблица» и номер ее указывают слева над первой частью таблицы, над другими частями пишут «Продолжение таблицы 1».

Цифровой материал, как правило, оформляют в виде таблиц в соответствии с рисунком 1.

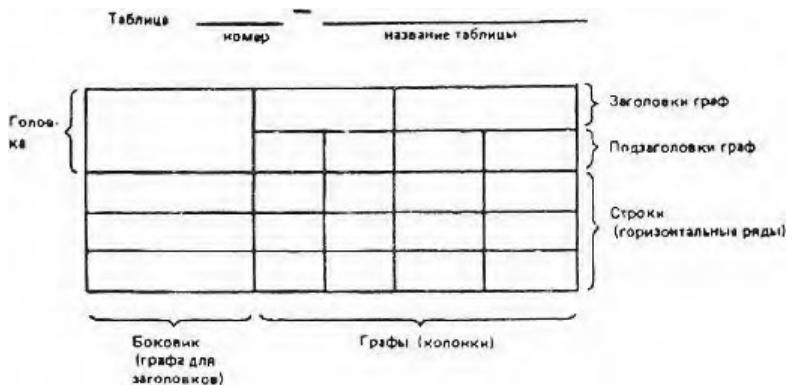


Рисунок 1– Пример таблицы

Если цифровые или иные данные в какой-либо строке таблицы не приводят, то в ней ставят прочерк.

Таблицы, за исключением таблиц приложений, следует нумеровать арабскими цифрами сквозной нумерацией.

Таблицы каждого приложения обозначают отдельной нумерацией арабскими цифрами с добавлением перед цифрой обозначения приложения.

Если в документе одна таблица, то она должна быть обозначена «Таблица 1» или «Таблица В. 1», если она приведена в приложении В.

Заголовки граф и строк таблицы следует писать с прописной буквы в единственном числе, а подзаголовки граф — со строчной буквы, если они составляют одно предложение с заголовком, или с прописной буквы, если они имеют самостоятельное значение. В конце заголовков и подзаголовков таблиц точки не ставят.

Таблицы слева, справа и снизу, как правило, ограничивают линиями. Допускается применять размер шрифта в таблице меньший, чем в тексте.

Разделять заголовки и подзаголовки боковика и граф диагональными линиями не допускается. Высота строк таблицы должна быть не менее 8 мм.

Заголовки граф, как правило, записывают параллельно строкам таблицы. При необходимости допускается перпендикулярное расположение заголовков граф.

Если строки или графы таблицы выходят за формат страницы, ее делят на части, помещая одну часть под другой или рядом, при этом в каждой части таблицы повторяют ее головку и боковик. При делении таблицы на части допускается ее головку или боковик заменять соответственно номером граф и строк. При этом нумеруют арабскими цифрами графы и (или) строки первой части таблицы.

Оформление таблиц в курсовой работе должно соответствовать ГОСТ 1.5 и ГОСТ 2.105.

Пример:

Таблица 1 – Результаты структурирования информации

№ элемента информации	Наименование элемента информации	Гриф конфиденциальности информации	Цена информации	Наименование источника информации	№ элемента информации
1	2	3	4	5	6

Продолжение таблицы 1

№ элемента информации	Наименование элемента	Гриф конфиденциальности информации	Цена информации	Наименование источника	№ элемента информации
-----------------------	-----------------------	------------------------------------	-----------------	------------------------	-----------------------

	информа- ции			информа- ции	
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>

Графическая часть курсовой работы (чертежи, схемы и т. п.) выполняется с соблюдением соответствующих государственных стандартов. Каждое приложение должно начинаться с нового листа с указанием сверху листа по центру слова «Приложение» и иметь тематический заголовок.

3 Организация выполнения и порядок руководства курсовыми работами

Руководство курсовыми работами должно поручаться наиболее квалифицированным преподавателям кафедры, обладающим методическим опытом и научной квалификацией. Для учета специфики курсовых работ по специальностям каждой кафедре необходимо разработать методические указания по выполнению курсовых работ.

Руководство курсовыми работами начинается с выдачи задания студентам. В этот период необходимым условием, обеспечивающим эффективность дальнейшего руководства, является индивидуальная беседа руководителя со студентом по заданию. В ходе беседы руководитель должен выяснить степень подготовленности студента к выполнению данного задания, рекомендовать необходимую литературу и информировать о порядке выполнения задания. В результате индивидуальной беседы может быть уточнена или выбрана студентом другая тема работы.

Задание выдается за подписью руководителя работы, датируется днем выдачи и регистрируется в кафедральном журнале.

В ряде случаев необходимо организовывать на кафедре чтение вводных лекций профессора или одного из опытных руководителей с целью разъяснения значения курсовой работы для данной дисциплины, требований, предъявляемых к работе.

В рамках отведенного для руководства курсовыми работами времени должны регулярно проводиться индивидуальные консультации.

Одной из важных форм руководства является предварительный просмотр выполненной курсовой работы. Если работа содержит экспериментальную часть, то руководитель, прежде всего, должен провести экспертизу этой части, а затем указать все ошибки, неточности по работе в целом.

После проверки выполнения студентом одного этапа работы, руководитель работы разрешает студенту перейти к следующему.

Заведующий кафедрой должен периодически проверять состояние работы, контролировать направленность и методику деятельности отдельных руководителей, давая на заседаниях кафедры соответствующие методические указания.

Работа перед сдачей руководителю подписывается студентом. Если работа удовлетворяет требованиям, предъявляемым к курсовым работам, она допускается к защите, о чем руководитель делает надпись на титульном листе.

4. Защита курсовых работ

Защита курсовой работы является обязательной формой проверки выполнения работы. Защита производится на заседании кафедры, научно-методического семинара кафедры, научной проблемной группы специальной комиссией, состоящей

обычно из 3 преподавателей кафедры, при непосредственном участии руководителя, в присутствии студентов. Результаты наиболее интересных курсовых работ могут быть доложены на научных конференциях.

Защита состоит в коротком докладе студента по выполненной работе и в ответах на вопросы присутствующих на защите. Научный руководитель зачитывает отзыв на курсовую работу студента (Приложение Д).

Результаты защиты курсовой работы, согласно действующему Положению о текущем контроле и промежуточной аттестации в СКФУ, оцениваются дифференцированной отметкой по пятибалльной системе. Оценка курсовой работы заносится в зачетную книжку студента и зачетно-экзаменационную ведомость (Приложение Д), составляемую в 2-х экземплярах, один из которых хранится на кафедре в течение всего срока обучения студента, другой представляется в дирекцию института.

Защита курсовых работ, предусмотренных учебным планом, проводится не позднее, чем за две недели до начала зачетно-экзаменационной сессии.

Студент, не представивший в установленный срок курсовую работу или не защитивший ее по неуважительной причине, считается имеющим академическую задолженность.

Курсовые работы, представляющие теоретический и практический интерес, следует представлять на конкурс в студенческие научные общества, конференции, отмечать приказом по университету.

Выполненные работы после их защиты должны храниться на кафедре в течение 2 лет, не считая года написания, затем работы, не представляющие для кафедры интерес, уничтожаются по акту.

Итоги выполнения курсовых работ ежегодно обсуждаются на кафедрах и по мере необходимости на Ученых советах институтов, а в отдельных случаях и на заседаниях Ученого Совета университета.

Приложение А

(обязательное)

УТВЕРЖДАЮ

Заведующий кафедрой
организации и технологии защиты информации
канд. техн. наук, доцент

В.И.

Петренко « ____ »

_____ 20__ г.

Институт Факультет математики и компьютерных наук им. Профессора
Н.И. Червякова _____

~~Кафедра~~ _____ Организации и технологии защиты информации

~~Направление~~ _____ Информационная безопасность

Профильная программа Комплексная система защиты информации на предпри-
_____ ятии

ЗАДАНИЕ на курсовую работу

студента	Иванов Иван Андреевич	
(фамилия, имя,		
отчество)	Комплексная система защиты информации	на
по дисциплине	предприятии	

1. Тема работы Разработка системы управления информационной безопасностью коммерческого предприятия

2. Цель _____

3. Задачи _____

4. Перечень подлежащих разработке вопросов:

а) по теоретической части _____

б) по аналитической части _____

5. Исходные данные:

а) по литературным источникам _____

б) по вариантам, разработанным преподавателем

в) иное _____

6. Список рекомендуемой литературы

7. Контрольные сроки представления отдельных разделов курсовой работы:

25 % - _____ «__» _____ 20__ г.

50 % - _____ «__» _____ 20__ г.

75 % - __ «__» __ 20__ г. 100 % - __ «__» __ 20__ г.

8. Срок защиты студентом курсовой работы «__» 20__ г. Дата выдачи задания «__» _____ 20__ г.

Руководитель курсовой работы канд. техн. наук, доцент _____ В.Е.
Рачков
(ученая степень, звание) (личная подпись) (инициалы, фамилия)

Задание принял(а) к исполнению студент(ка) очной формы обучения
4 курса ИНБ-м-о-14-1 группы _____ И.А. Иванов
(личная подпись) (инициалы, фамилия)

Приложение Б

(обязательное)

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГАОУ ВПО «СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Факультет математики и компьютерных наук им. Профессора Н.И.Червякова
КАФЕДРА ОРГАНИЗАЦИИ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ

КУРСОВАЯ РАБОТА

по дисциплине

«Комплексная система защиты информации на предприятии» на тему:
**«РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТЬЮ КОММЕРЧЕСКОГО ПРЕДПРИЯТИЯ»**

Выполнил:

Иванов Иван Андреевич
студент 4 курса группы ИНБ-м-о-14-1
направления «Информационная
безопасность» очной формы обучения

(подпись)

Руководитель работы: Рачков

Валерий Евгеньевич канд. техн. наук,
доцент кафедры ОТЗИ

Работа допущена к защите _____
(подпись руководителя) (дата)

Работа выполнена и
защищена с оценкой

Дата защиты

Члены
комиссии:

_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
(должность)	(подпись)	(И.О. Фамилия)

Ставрополь, 2018 г.

Приложение В (обязательное) Оглавление

Введение.....	3
1 Обзор существующих методов отслеживания установленного программного обеспечения на предприятии.....	4
1.1 Понятие отслеживания установленного программного обеспечения.....	5
1.2 Инвентаризация программного обеспечения.....	9
1.3 Аудит программного обеспечения.....	12
1.4 Выводы по главе.....	16
2 Способы отслеживания установленного программного обеспечения в информационной среде предприятия.....	17
2.1 Обзор существующих программ отслеживания установленного программного оборудования.....	17
2.2 Realité: реальный контроль.....	26
2.3 Выводы по	

главе.....	29
3 Разработка программы для инвентаризации и учета программ на компьютерных сетях «учет программного обеспечения»	31
3.1 Понятие и способы применения программы «Учет программного обеспечения».....	32
3.2 Существующие виды программы и её достоинства.....	31
25	
3.3	Выводы
главе.....	по 33
Закключение.....	35
Список использованных источников.....	37

Приложение Г

(обязательное)

Список использованных источников В.1 Нормативно-руководящие документы

1. Федеральный закон от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон «О коммерческой тайне» от 29.07.2004 г. №98-ФЗ.
3. Федеральный закон «О персональных данных» от 27.07.2006 г. №152-ФЗ.
4. Федеральный закон «О техническом регулировании» от 27.12.2002 г. №184-ФЗ.
5. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
6. «Доктрина информационной безопасности Российской Федерации» (Утв. Указ Президента РФ от 05.12.2016 г. № 646).
7. «Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ» Утв. Указ Президента РФ от 12.12.2014г № К1274).

8. «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» (утв.

Президентом РФ 24.07.2013, №Пр-1753).

9. ГОСТ РО 0043-001-2010 «Защита информации. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры.

Термины и определения».

10. ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов

информатизации. Программа и методики аттестационных испытаний».

11. ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов

информатизации. Общие положения».

12. Специальные требования и рекомендации по технической защите

27

конфиденциальной информации (СТР-К) (Утв. Гостехкомиссией в 2002 г).

13. Сборник временных методик оценки защищённости конфиденциаль-

ной информации от утечки по техническим каналам. (Утв. Гостехкомиссией в 2001 г)

14. Приказ ФСТЭК от 18.02.2013г №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

15. Приказ ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении Состав и содержания организационных и технических мер по

обеспечению без- опасности персональных данных при их обработке в информационных системах персональных данных».

16. ИСО/МЭК 27002 Информационные технологии. Методы и средства обеспечения безопасности. Практические правила управления ИБ.

17. Устав организации

В.2 Книги с различным количеством авторов -количество

авторов не более трех:

18. Ворона В.А. Комплексные интегрированные системы обеспечения безопасности: учебное пособие/ Ворона В.А., Тихонов В.А.— Электрон.текстовые данные.— М.: Горячая линия - Телеком, 2013.— 160 с.

19. . Сердюк В. А. Организация и технологии защиты информации: об- наружение и предотвращение информационных атак в автоматизированных си- стемах предприятий. М.: ГУ-ВШЭ, 2013 — ISBN 978-5-7598-0698-1 — 576 с.

20. Завгородний В.А. Комплексная защита информации в компьютер-
ных системах. – М.: Логос, 2003. – 264 с.

21. Конеев И.Р. Информационная безопасность предприятий. - СПб.: БХВ-Петербург, 2013.- 752 с.

22. Ярочкин В.И. Информационная безопасность. – М.: Академический Проект: Фонд "Мир", 2013. – 640 с.

23. Гришина Н.В. Комплексная система защиты информации на пред-
приятии. – М.: Форум, 2014. – 240 с.

24. Шаньгин В.Ф. Комплексная защита информации в корпоративных

системах. – М.: Инфра–М, Форум, 2010. – 592 с.

25. Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии. – М. Издательский дом "Академия", 2014. – 416 с.

-количество авторов не более четырех:

26. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия: Учебное пособие. – М.: Издательско-торговая корпорация «Дашков и Ко », 2004. – 336 с.

В.3 Тезисы доклада, сообщения, доклад, другие материалы совещаний (конференций)

27. Макеев К.И. Комплексная система защиты информации в системах

электронного документооборота. В сборнике: Международная научно-техническая конференция молодых ученых БГТУ им. В.Г. Шухова Белгородский государственный технологический университет им. В.Г. Шухова. 2015. С. 2902-2906.

28. Бисюков В.М., Сагдеев К.М., Кузнецов Н.И. Анализ состояния и выбор

стратегии технического обслуживания в системах комплексной защиты информации для распределенных информационных систем. В сборнике: Актуальные проблемы современной науки IV Международная научно-практическая конференция. 2015. С. 292-296.

29. Ларионов И.П., Хорев П.Б. Особенности представления знаний в экспертной системе поддержки проектирования комплексной системы защиты информации. В сборнике: Современные проблемы гуманитарных и

естественных наук Материалы XXIV международной научно-практической конференции. Научноинформационный издательский центр "Институт стратегических исследований". 2015. С. 42-48.

30. Оценка эффективности комплексных систем защиты информации Леонтьева Е.М. В сборнике: Современные инновации в науке и технике. Сборник научных трудов 4-ой Международной научно-практической конференции: В 4-х томах. Ответственный редактор Горохов А.А.. 2014. С. 378-379.

В.4 Статьи из журналов и периодических сборников, продолжающихся сборников, ежегодников:

31. Белова Е.А., Зарубин В.С. Некоторые подходы к формированию цели управления механизмами защиты информации в комплексных системах без- опасности. Охрана, безопасность, связь. 2016. №1-1. С. 51-53.

32. Овчинников А.О. Подходы к комплексной системе защиты информации в органах внутренних дел. Актуальные проблемы права и государства в XXI веке. 2015. №7-5. С. 169-174.

33. Чаус Е.А. Особенности построения комплексных систем защиты ин-

формации в распределенных корпоративных сетях. Успехи современной науки и образования. 2016. Т. 2. № 4. С. 107-109.

34. Тараскин М.М., Коваленко Ю.И. Методика исследования угроз, уязвимостей и рисков в организации. Безопасность информационных технологий. 2013. №1. С. 124-125.

35. Тараскин М.М., Коваленко Ю.И. Вербальная формулировка подхода к построению оптимальной системы комплексной защиты информации в организации. Безопасность информационных технологий. 2013. №1. С. 122-123.

В.5 Источники из Интернета

36. Федеральная служба по техническому и экспортному контролю. Документы. - <http://fstec.ru/>.

37. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. - <https://rkn.gov.ru/>.

38. Гришина Н.В. Организация комплексной системы защиты информации. - http://www.razlib.ru/kompyutery_i_internet/organizacija_kompleksnoi_sistemy_zashity_informacii/

39. Security Lab - <http://www.securitylab.ru/>.

40. Threatpost - <https://threatpos>.

41. Anti-Malware - <https://www.anti-malware.ru/>.

42. Блог Алексея Лукацкого - <http://lukatsky.blogspot.it/>. 30

43. Блог Евгения Царева <https://www.tsarev.biz/>.

44. Журнал «Information Security» -
<http://www.itsec.ru/articles2/allpub>- Сайт liks.
производителя АПКШ «Континент» - <https://www.securitycode.ru/>.

Приложение Д

(обязательное)

Отзыв на курсовую работу студента/ки
курса Ф.И.О.

тема Актуальность: курсовая работа

посвящена В первой главе

Вторая глава

Выводы, сделанные в Заключение, соответствуют целям, поставленным во
Введении.

Проанализирован объем литературы...

За время работы студент/ка проявил/а себя как.....

Таким образом, работа выполнена на ... уровне, соответствует требова-
ниям, предъявляемым к курсовым работам, и заслуживает ... оценки.

Научный руководитель степень, звание, должность место работы
Ф.И.О.

Печать "...."...

201...г.

Приложение Е

Темы курсовых работ

1. Исследование возможностей программных комплексов для организации юридически значимого конфиденциального электронного документооборота на предприятии.

2. Разработка политики информационной безопасности предприятия.
3. Разработка рекомендаций по совершенствованию комплексной системы защиты информации путём повышения защищённости локальной вычислительной сети предприятия.
4. Анализ функциональных возможностей систем удалённой биометрической аутентификации пользователей информационных систем.
5. Разработка технико-экономического обоснования комплексной системы защиты коммерческой тайны предприятия.
6. Разработка рекомендаций по управлению рисками информационной безопасности коммерческого предприятия.
7. Сравнительный анализ подходов к финансовой оценке угроз информационной безопасности предприятия.
8. Разработка рекомендаций по защите компьютерной сети предприятия на основе продуктов Secret Net.
9. Совершенствование комплексной системы защиты информации предприятия на основе внедрения подсистемы разграничения доступа в информационной системе.
10. Разработка рекомендаций по защите информационной системы предприятия от внешних угроз информационной безопасности с использованием АПКШ «Континент».
11. Разработка системы управления информационной безопасностью коммерческого предприятия.
12. Разработка модели угроз информационной безопасности коммерческого предприятия.
13. Разработка рекомендаций по совершенствованию пропускного режима на предприятии на основе идентификации по трёхмерным моделям лиц.

14. Исследование возможностей DLP-систем по выявлению и предотвращению угроз информационной безопасности со стороны персонала предприятия.
15. Разработка системы контроля и управления доступом на предприятие на основе биометрической идентификации.
16. Исследование влияния кадровой политики на уровень информационной безопасности предприятия.
17. Разработка рекомендаций по проведению внутреннего аудита комплексной системы информационной безопасности коммерческого предприятия.
18. Разработка и обоснование организационно-штатной структуры подразделения по защите коммерческой тайны на предприятии.
19. Анализ влияния рисков со стороны персонала на информационную безопасность предприятия.
20. Разработка модели нарушителя информационной безопасности коммерческого предприятия.
21. Исследование инструментов минимизации ущерба от нарушения информационной безопасности на коммерческом предприятии.
22. Исследование и оценка влияния критически важной информационной инфраструктуры организации на организацию защиты информации
23. Технологии моделирования систем комплексной защиты информации предприятия в объектно-ориентированной среде.