Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»

КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

КНИГА 35

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Учебное пособие к выполнению курсовой работы

Под редакцией профессора М. Ю. Монахова

Владимир 2023

УДК 004.056
ББК 16.8
У67

Редактор серии – доктор технических наук, профессор М. Ю. Монахов

Автор-составитель А. В. Тельный

Рецензенты:
Доктор технических наук, профессор
профессор кафедры радиотехники и радиосистем
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых
А. Г. Самойлов

Кандидат технических наук
проректор по цифровому развитию и информационной безопасности
Владимирского института развития образования
имени Л. И. Новиковой
Д. В. Мишин

Издается по решению редакционно-издательского совета ВлГУ

Управление информационной безопасностью : учеб. пособие
У67 к выполнению курсовой работы / авт.-сост. А. В. Тельный ; под ред. проф. М. Ю. Монахова ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир : Изд-во ВлГУ, 2023. – 223 с. – (Комплексная защита объектов информатизации. Кн. 35). – ISBN 978-5-9984-1791-7.

Изложен систематизированный материал для написания курсовой работы в рамках учебной дисциплины «Управление информационной безопасностью», посвященный комплексной оценке состояния информационной безопасности автоматизированной информационной системы (АИС) предприятия. Представлены основные методологические подходы к описанию и обследованию состояния защищенности АИС. Предложено шесть вариантов заданий.

Предназначено для студентов вузов направления подготовки 10.04.01 «Информационная безопасность» и специальности 10.05.04 «Информационно-аналитические системы безопасности» очной формы обучения.

Рекомендовано для формирования профессиональных компетенций в соответствии с ФГОС ВО.

Ил. 5. Табл. 55. Библиогр.: 28 назв.

УДК 004.056
ББК 16.8

ISBN 978-5-9984-1791-7

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Задача изучения дисциплины «Управление информационной безопасностью» – освоение принципов реализации и основных подходов оптимального управления различными механизмами информационной безопасности в автоматизированных информационных системах. В процессе выполнения курсовой работы изучаются следующие вопросы:

– основные руководящие документы и показатели эффективности системы защиты информации АИС;

– цели, стратегии и политика информационной безопасности;

– функции управления и процессный подход к управлению информационной безопасностью;

– система ответственности в области информационной безопасности;

– оценивание риска в информационных системах;

– оптимальный выбор средств комплексной системы защиты информации от возможных угроз информационной безопасности;

– практика применения программных средств проведения аудита информационной безопасности;

– концепция построения системы безопасности АИС предприятия.

Цель выполнения курсовой работы – овладение навыками практической деятельности в области моделирования и анализа технических средств управления информационной безопасностью в АИС и службой безопасности на предприятии с использованием средств вычислительной техники, формирование умения использовать соответствующее специализированное программное обеспечение.

В рамках курсовой работы изучаются и выявляются угрозы информационной безопасности в АИС на типовом предприятии, имеющем в своем составе разные виды конфиденциальной информации. В качестве исходных данных обучающиеся получают 10 вариантов

(в том числе в электронном виде) описаний АИС типовых организаций: описание и поэтажные планы размещения средств вычислительной техники на объекте защиты; описание организационно-штатной (далее – оргштатная) структуры объекта; описание информационной инфраструктуры и размещения информационных ресурсов ограниченного доступа в АИС (в пособии приведены шесть вариантов заданий).

В ходе выполнения работы необходимо:

– сформировать исполнительскую документацию для организации локальной вычислительной сети (ЛВС) АИС объекта защиты;

– описать структуру распределения аппаратных и информационных ресурсов в ЛВС АИС;

– сформировать матрицу и модель доступа к информационным ресурсам АИС;

– классифицировать АИС предприятия по требованиям руководящих документов Федеральной службы по техническому и экспортному контролю (ФСТЭК) России;

– сформировать модель нарушителя информационной безопасности в АИС на предприятии;

– определить класс защищенности информационной системы и состав базовых мер защиты информации в АИС.

Заключительный этап работы – проведение аудита информационной безопасности АИС с использованием специализированного бесплатного программного обеспечения Microsoft Security Assessment Tool.

Список используемых сокращений

АВЗ – антивирусная защита
АИС – автоматизированная информационная система
АНЗ – анализ защищенности информации
АРМ – автоматизированное рабочее место
АС – автоматизированная система
АСУ – автоматизированная система управления
БД – база данных
ГИС – государственная информационная система
ГИС ПДн – государственная информационная система обработки персональных данных
ЗИ – защита информации
ЗИС – защита информационной системы
ЗНИ – защита машинных носителей информации
ЗСВ – защита среды виртуализации
ЗТС – защита технических средств
ИАФ – идентификация и аутентификация субъектов и объектов доступа
ИБ и ТЗИ – информационная безопасность и техническая защита информации
ИС – информационная система
ИСПДн – информационная система персональных данных
ИТКС – информационно-телекоммуникационная система
ИТУ – инженерно-техническая укрепленность
КИ – конфиденциальная информация
КПиОР – контрольно-пропускной и объектовый режим
КПП – контрольно-пропускной пункт
КРИВС – корпоративная распределенная информационно-вычислительная сеть
КТ – коммерческая тайна
ЛВС – локальная вычислительная сеть
ЛС – локальная сеть
НВ – несанкционированное воздействие
НСД – несанкционированный доступ
ОДС – оперативно-диспетчерская служба

ОМТиХО – отдел материально-технического и хозяйственного обеспечения
ОПС – ограничение программной среды
ОПС – охранно-пожарная сигнализация
ОС – операционная система
ОС – охранная сигнализация
ОТ и ТБ – охрана труда и техника безопасности
ОТС – охранно-тревожная сигнализация
ОЦЛ – обеспечение целостности информационной системы и информации
ПК – персональный компьютер
ПО – программное обеспечение
ПРБ – профиль риска для бизнеса
ПЦО – пункт централизованной охраны
ПЭВМ – персональная электронно-вычислительная машина
РД – руководящий документ
РСБ – регистрация событий безопасности
СБ – служба безопасности
СВН – система видеонаблюдения
СВТ – средства вычислительной техники
СЗИ – средство(а) защиты информации
СКЗИ – криптографические средства защиты информации
СКС – структурированные кабельные системы
СКУД – система контроля управления доступом
СОС – система охранной сигнализации
СОТ – система охранная телевизионная
ТСО – техническое средство охраны
УЗ – уровень значимости
УПД – управление доступом субъекта доступа к объектам доступа
ФСБ России – Федеральная служба безопасности Российской Федерации
ФСТЭК России – Федеральная служба по техническому и экспортному контролю Российской Федерации
ЦОД – центр обработки данных
DiD – стратегии эшелонированной защиты
DiDI – индекс эшелонированной защиты

Бланк и структура задания на курсовую работу

Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)

Кафедра информатики и защиты информации

«УТВЕРЖДАЮ»
Заведующий кафедрой_____
_____

«___» _____ 20__г.

Задание на курсовую работу по дисциплине
«Управление информационной безопасностью»
Вариант №_____

студенту группы

_____

(номер группы, ФИО)

Тема работы: Комплексная оценка состояния информационной безопасности АИС предприятия (по вариантам) ____

Срок сдачи законченной работы: «___» _____20__ г.

Исходные данные к работе: выданные планировки, описание, оргштатная структура объекта, описание информационной инфраструктуры АИС по вариантам в электронном виде. Бесплатное, свободно распространяемое ПО Microsoft Security Assessment Tool для оценки состояния информационной безопасности АИС предприятия

Основные механизмы и процедуры, которые необходимо реализовать: разработка исполнительской документации для локальной вычислительной сети АИС объекта защиты; описание структуры распределения аппаратных и информационных ресурсов в ЛВС АИС объ-

екта защиты; формирование матрицы и модели доступа к информационным ресурсам АИС; классификация АИС предприятия по требованиям руководящего документа ФСТЭК России от 30 марта 1992 г.; формирование модели нарушителя информационной безопасности в АИС на предприятии; определение класса защищенности информационной системы и состава базовых мер защиты информации; проведение аудита информационной безопасности АИС с использованием специализированного программного обеспечения Microsoft Security Assessment Tool.

Примерное содержание пояснительной записки следующее:

– титульный лист;

– задание на курсовой проект/работу;

– оглавление;

– реферат (аннотация);

– введение;

– разделы 1 – 7;

– заключение;

– список использованных источников.

Раздел 1. Разработка исполнительской документации для локальной вычислительной сети АИС объекта защиты:

– планировка объекта и описание состояния инженерно-технического укрепления элементов строительных конструкций;

– экспликация помещений на планировках, описание оргштатной структуры объекта и основных задач структурных подразделений;

– описание оргштатной структуры службы безопасности и выполняемых ею задач; краткое описание административно-управленческого персонала объекта;

– описание структуры защищаемой информации (какие информационные ресурсы где находятся и какой степени конфиденциальности);

– поэтажные планы объекта;

– генплан расположения объекта на местности;

– поэтажные планы расположения по помещениям средств вычислительной техники;

– пояснительная записка с обоснованием выбора топологии ЛВС организации;

– пояснительная записка с обоснованием выбора пассивного и активного сетевого оборудования ЛВС организации;

– в пояснительных записках отражаются состав ЛВС предприятия (организации), их топология, протоколы, распределение ресурсов и прав доступа.

Основные характеристики ЛВС:

– территориальная протяженность сети (длина общего канала связи);

– максимальная скорость передачи данных;

– максимальное число автоматизированных систем (АС) в сети;

– максимально возможное расстояние от рабочих станций до коммутаторов (маршрутизаторов) в сети;

– топология сети;

– вид физической среды передачи данных;

– максимальное число каналов передачи данных;

– тип передачи сигналов (синхронный или асинхронный);

– метод доступа абонентов в сеть;

– структура программного обеспечения сети;

– возможность передачи речи и видеосигналов;

– условия надежной работы сети;

– возможность связи ЛВС между собой и с сетью более высокого уровня;

– возможность использования процедуры установления приоритетов при одновременном подключении абонентов к общему каналу;

– схемы поэтажных планов размещения средств вычислительной техники, соединительных кабелей телекоммуникаций ЛВС, пассивного и активного сетевого оборудования ЛВС;

– структурная схема ЛВС в организации: серверы, рабочие станции, пассивное и активное сетевое оборудование, вспомогательные периферийные устройства с указанием номеров ПК и IP-адресации;

– схемы прокладки кабеля оптоволоконной сети и её оборудования (при наличии);

– устройства Wi-Fi (схема зон охвата помещений здания).

Раздел 2. Описание структуры распределения аппаратных и информационных ресурсов в ЛВС АИС объекта защиты:

– описания подключения компьютеров к сетевому оборудованию и связь сетевого оборудования между собой;

– описание адресного пространства локальной сети (ЛС);

– описание учета аппаратных технических средств информатизации для серверов и рабочих станций;

– описание учета аппаратных технических средств активного сетевого оборудования;

– описание учета аппаратных периферийных технических средств;

– описание учета программного обеспечения, установленного на компьютерах ЛВС;

– подтверждение лицензионной чистоты программного обеспечения;

– документы по организации доступа к глобальным сетям и сети Интернет.

Раздел 3. Формирование матрицы и модели доступа к информационным ресурсам АИС:

– на каждом компьютере ЛВС (где находятся информационные ресурсы разной степени конфиденциальности) определить, какие информационные ресурсы будут свободно использоваться всеми сотрудниками организации и всеми посетителями, а какие ресурсы будут иметь ограниченный доступ;

– на каждом компьютере ЛВС определить применяемую систему организации распределения доступа и необходимые программно-аппаратные средства организации доступа;

– для каждого компьютера и каждого пользователя этого компьютера – сотрудника организации составить модели доступа к информационным ресурсам, выбрать способы и технические средства организации распределения доступа;

– определить необходимые программные средства организации удаленного доступа.

Раздел 4. Классификация АИС предприятия по требованиям руководящего документа ФСТЭК России. Состоит из таблицы классификации АИС по классам защищённости согласно документу ФСТЭК России от 30 марта 1992 г. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

Раздел 5. Формирование модели нарушителя информационной безопасности в АИС на предприятии:

– пояснительная записка с обоснованием выбора актуальных нарушителей для заданного объекта защиты и определением их типов;

– таблица определения актуальных нарушителей при реализации угроз безопасности информации и соответствующих им возможностей для объекта защиты;

– таблица определения актуальных способов реализации угроз безопасности информации, соответствующих им видов нарушителей и их возможностей для объекта защиты.

Раздел 6. Определение класса защищенности информационной системы и состава базовых мер защиты информации для соответствующего класса защищенности государственных информационных систем (ГИС) (не содержащих сведений, составляющих государственную тайну) согласно приказам ФСТЭК России № 17 (2013 г.) и № 27 (2017 г.):

– пояснительная записка с обоснованием оценки класса защищенности для каждой информационной системы (ИС) объекта защиты в соответствии с приложением 1 приказа ФСТЭК России № 17 (2013 г.) в редакции приказа ФСТЭК России № 27 (2017 г.);

– анализ состава мер защиты информации и их базовых наборов для соответствующего класса защищенности информационной системы по методике приложения 2 приказа ФСТЭК России № 17 (2013 г.) в редакции приказа ФСТЭК России № 27 (2017 г.).

Раздел 7. Проведение аудита информационной безопасности АИС с использованием специализированного программного обеспечения Microsoft Security Assessment Tool (MSAT). Отчет MSAT (в электронном виде) о результатах аудита защищаемой АИС и рекомендации по повышению информационной безопасности защищаемой АИС в составе отчета MSAT.

Дата выдачи задания: «___»_____20___ г.
Руководитель _____/_____/

Задание принял к исполнению _____/_____/
(подпись) (инициалы и фамилия)

Глава 1. РАЗРАБОТКА ИСПОЛНИТЕЛЬСКОЙ ДОКУМЕНТАЦИИ ДЛЯ ЛВС АИС ОБЪЕКТА ЗАЩИТЫ

1.1. Общие положения

В качестве исходного задания студентам по вариантам выдаётся:

– описание объекта защиты (здания), его планировка и описание состояния инженерно-технического укрепления элементов строительных конструкций;

– экспликация помещений на планировках; описание оргштатной структуры объекта и основных задач структурных подразделений;

– описание оргштатной структуры службы безопасности и выполняемых ею задач; краткое описание административно-управленческого персонала объекта;

– описание структуры защищаемой информации (какие информационные ресурсы где находятся и какой степени конфиденциальности);

– поэтажные планы объекта;

– генплан расположения объекта на местности;

– поэтажные планы расположения по помещениям средств вычислительной техники.

Допускается использовать студентам собственные исходные данные, аналогичные вышеприведённым и соответствующие реальным объектам. Например, это может быть предприятие, где студент проходит практику или работает. **Однако при этом необходимо обеспечить обезличивание информации об описываемой АИС и распределении информационных ресурсов в ней.**

Для проектирования ЛВС проведите исследование условий функционирования локальных сетей разного уровня. Этот шаг решающий для определения параметров, в пределах которых должен работать студент. Существующие условия на предприятии формируют основу для конструирования любой сети. Задокументируйте требования к сети.

Сколько компьютеров используется в настоящий момент, а сколько предполагается использовать в будущем?

Какие типы компьютеров объединяются в сеть?

Какие специальные периферийные устройства требуются?

Будет ли локальная сеть подключена к мейнфрейму или глобальной сети?

Какое программное обеспечение (ПО) используется или предполагается к использованию?

Какой тип административного контроля требуется?

Какой уровень разделения ресурсов потребуется?

Выберите сетевую операционную систему (NOS). Она диктует, какой потребуется тип оборудования для файлового сервера и какие транспортные протоколы будут поддерживаться. Убедитесь, что сетевая операционная система может отвечать существующим и будущим сетевым требованиям и будет поддерживаться в течение длительного времени. Также определите административные расходы, которые может вызвать операционная система. Спланируйте логическую сеть. Этот шаг включает в себя выбор транспортного протокола и технологий связи данных, при необходимости – разделение сети на подсети и выбор зон безопасности.

Определите сетевую технологию. Часто это самый трудный шаг, поскольку планируется неизвестное. Определение нагрузки клиентов и того, какие технологии будут поддерживать эту нагрузку, затруднительно, когда необходимо оценить емкость. Например, хотя сеть Token Ring обеспечивает большую скорость передачи, чем сеть Ethernet, рабочие станции должны ждать маркера, чтобы начать передачу, в результате чего сеть Ethernet может показаться более быстрой. Сеть Token Ring при добавлении клиентов загружается простым, линейным, образом, в то время как перегруженная сеть Ethernet может вообще прекратить свое функционирование.

Спланируйте физическое расположение. Окружение, так же как и выбранная архитектура, диктует, какой кабель и какая топология должны быть использованы. Пользовательские и корпоративные требования определяют, как и где должны располагаться файловые серверы, концентраторы и маршрутизаторы.

Выберите аппаратную платформу файлового сервера.

Определите требования к хранению информации. Это трудно сделать в случае новой установки, поскольку нет никакой исходной информации. Используйте рекомендации, данные для выбранной сетевой операционной системы и данные производителя, полученные с оборудованием для файлового сервера. Планируйте удваивать емкость дисков каждый год. Убедитесь, что имеется достаточно оперативной памяти для потребностей в хранении.

Спланируйте поддержку клиентов. Чтобы продуктивно использовать базы данных, браузер и другие основные приложения, большинство рабочих мест должно быть оснащено компьютером по крайней мере с Intel-совместимым процессором, оперативной памятью не менее чем 4 Гбайт, совместимым оборудованием и программным обеспечением. Убедитесь, что маршрутизаторы поддерживают все протоколы, которые потребуются в сети.

Порядок создания исполнительской документации для локальной вычислительной сети АИС объекта защиты следующий:

– выбор типа топологии сети и методов доступа (выбор сетевой архитектуры);

– планирование физической структуры сети с привязкой к предприятию;

– выбор подсетей и их архитектуры **(должно быть минимум две подсети и одна подсеть с использованием беспроводных технологий Wi-Fi)**;

– выбор сетевой операционной системы в каждой из подсетей;

– выбор сетевого аппаратного обеспечения;

– выбор сетевого программного обеспечения;

– выбор периферийного оборудования, необходимого для функционирования структурных подразделений организации при следующих условиях:

– не менее одного принтера в служебный кабинет с ПК и не менее одного сканера на структурное подразделение (отдел);

– использование IP-телефонии (не менее одного аппарата в организации);

– разработка спецификаций на сеть (полный перечень аппаратного активного и пассивного сетевого оборудования и программного обеспечения с указанием количества и фирм-производителей).

В ходе выполнения курсовой работы необходимо *составить комплект исполнительской документации для локальной вычислительной сети АИС объекта защиты* в следующем составе:

– пояснительная записка с обоснованием выбора топологии ЛВС организации;

– пояснительная записка с обоснованием выбора пассивного и активного сетевого оборудования ЛВС организации;

– в пояснительных записках отражаются состав ЛВС предприятия (организации), их топология, протоколы, распределение ресурсов и прав доступа.

Основные характеристики ЛВС:

– территориальная протяженность сети (длина общего канала связи);

– максимальная скорость передачи данных;

– максимальное число АС в сети;

– максимально возможное расстояние от рабочих станций до коммутаторов (маршрутизаторов) в сети (для категории 5е – не более 90 м);

– топология сети;

– вид физической среды передачи данных;

– максимальное число каналов передачи данных;

– тип передачи сигналов (синхронный или асинхронный);

– метод доступа абонентов в сеть;

– структура программного обеспечения сети;

– возможность передачи речи и видеосигналов;

– условия надежной работы сети;

– возможность связи ЛВС между собой и с сетью более высокого уровня;

– возможность использования процедуры установления приоритетов при одновременном подключении абонентов к общему каналу;

– схемы поэтажных планов размещения средств вычислительной техники, соединительных кабелей телекоммуникаций ЛВС, пассивного и активного сетевого оборудования ЛВС;

– структурная схема ЛВС в организации: серверы, рабочие станции, пассивное и активное сетевое оборудование, вспомогательные периферийные устройства с указанием номеров ПК и IP-адресации;

– схемы прокладки кабеля оптоволоконной сети и её оборудования (при наличии);

– устройства Wi-Fi (схема зон охвата помещений здания).

При составлении исполнительской документации (так как она не является проектом ЛВС) не требуется оформления чертежей, их рамок и штампов.

1.2. Пример описания исполнительской документации для ЛВС АИС объекта защиты

ООО «Пример» занимается производством различных форм из силикона (для кулинарии, творчества, материалы для маникюрных салонов, ортопедические стельки, медицинские протезы). Продукция изготавливается на заказ. Заказы принимаются через сайт продаж завода по индивидуальным меркам клиента.

Объект – производственно-сбытовая химическая организация (торговля и маркетинг) ООО «Пример», занимающая 2-й и 3-й этажи трехэтажного кирпичного здания с дневным постом охраны на 1-м этаже (рис. 1.1). Охранно-пожарная сигнализация (ОПС) 2-го и 3-го этажей сводится в помещение 6 3-го этажа. В здании 1-й этаж занимают (арендуют) прочие «не охраняемые» собственники. Перекрытия полов и потолков капитальные, из железобетонных панелей. Имеется деревянный люк на плоскую крышу здания.

Все внутренние двери деревянные, филенчатые, полнотелые. Двери в служебные кабинеты и бухгалтерию, кассу, архив, канцелярию, серверную и другие имеют по одному врезному замку. Двери в холлах, коридорах, тамбурах остекленные в верхней половине и запорных устройств не имеют.

Все внутренние перегородки и стены (кроме наружных по периметру здания) гипсокартонные, каркасные или в кирпич (полкирпича), не капитальные. Во всех служебных кабинетах имеются персональные компьютеры, на складе – дорогостоящие материальные ценности. В помещении 1 и помещении кассы установлены сейфы массой 150 – 200 кг без крепления к полу и стенам. Кабинет 1 – защищаемое выделенное помещение с хранением информации, составляющей коммерческую тайну.

Двери: Д1 – дверь деревянная, полнотелая, филенчатая, с одним врезным замком.

Окна: О1 – окно пластиковое, с двойным остеклением, без защитных пленок, решетки отсутствуют;

О2 – окно пластиковое, с двойным остеклением, без защитных пленок, решетки отсутствуют;

О3 – окно пластиковое, с двойным остеклением, без защитных пленок, решетка со стороны помещения из прутка D = 12 мм, размер ячейки 200 × 200 мм.

Экспликация помещений объекта

2-й этаж:

1 – канцелярия;

2 – служебный кабинет;

3 – служебный кабинет;

4 – бухгалтерия с кассой;

5 – серверная;

6 – служебный кабинет;

7 – архив.

3-й этаж:

1 – кабинет руководителя;

1а – приемная;

2 – служебный кабинет;

3 – склад;

4 – служебный кабинет;

5 – служебный кабинет;

6 – служебный кабинет;

7 – коридор.

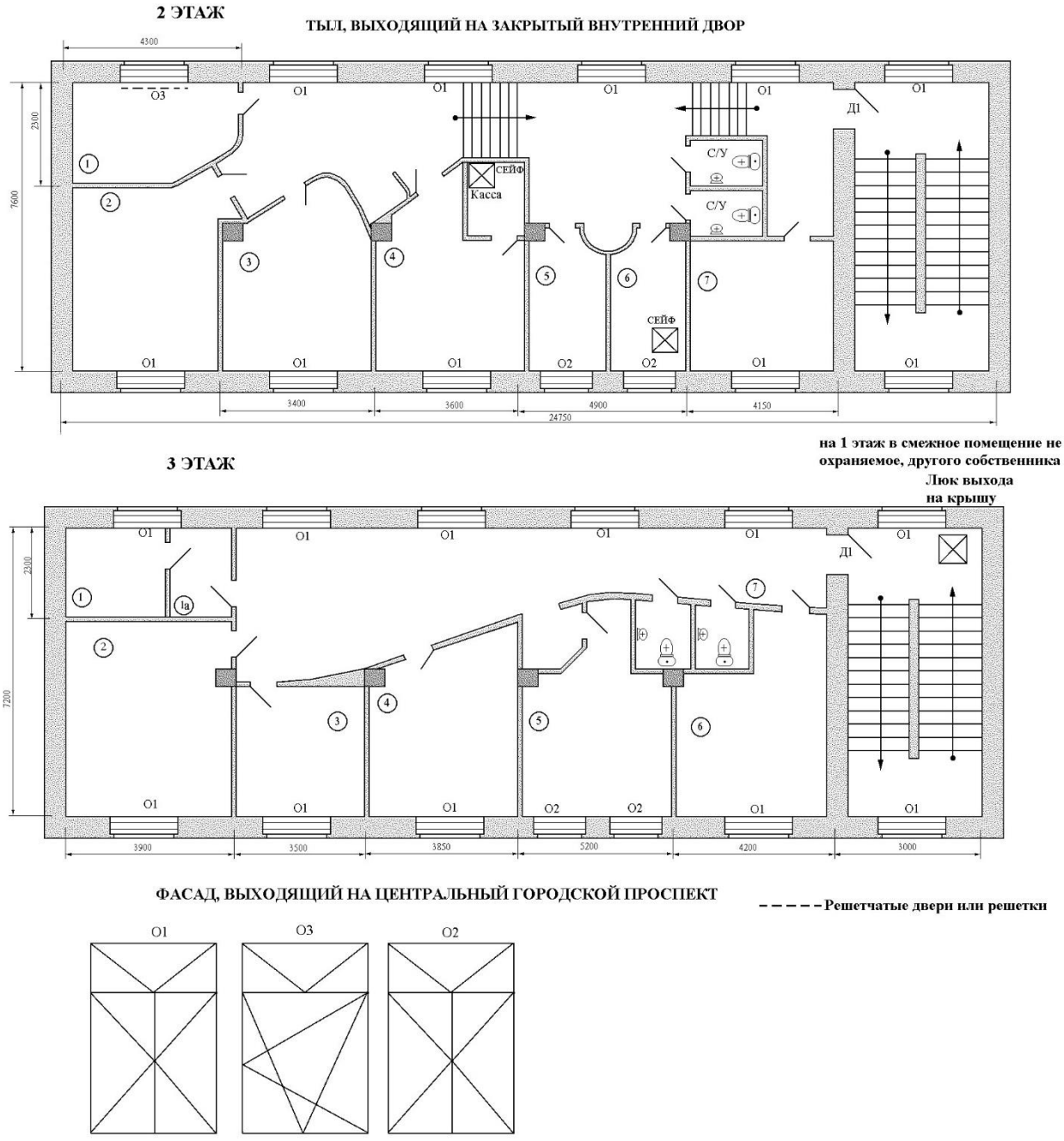

Рис. 1.1. Поэтажный план объекта

Структура организации следующая (табл. 1.1). Во главе ООО «Пример» стоит генеральный директор (каб. 1 на 3-м этаже), у которого один заместитель по экономике.

Непосредственно руководителю подчиняется:

– канцелярия (каб. 1 на 2-м этаже): организация делопроизводства, документооборота, архивного дела, подготовка и оформление документов, контроль за прохождением и исполнением документов в организации. В штате – зав. канцелярией (каб. 1 на 2-м этаже) и секретарь (в приемной – пом. 1а), зав. архивом (пом. 7 на 2-м этаже);

– служба безопасности (СБ) (пом. 6 на 2-м этаже, пом. 4, 5 на 3-м этаже): охрана собственности и защита персонала от противоправных посягательств, координация действий сотрудников и структур завода по вопросам обеспечения безопасности, защита от несанкционированного доступа к закрытой информации о персонале и деятельности завода, сбор, обработка и анализ конфиденциальной информации среди персонала завода, охрана коммерческой тайны. В штате – начальник службы безопасности (каб. 4 на 3-м этаже) и подразделения: группа охраны и режима – ст. инспектор (каб. 4 на 3-м этаже); группа режима конфиденциальной информации (КИ) – один инспектор (каб. 1 – канцелярия); группа информационной безопасности и технической защиты информации (ИБ и ТЗИ) – один администратор безопасности (каб. 4 на 3-м этаже), ст. инспектор и инспектор (каб. 5 на 3-м этаже), аналитик (каб. 5 на 3-м этаже); ст. юрисконсульт по безопасности (каб. 5 на 3-м этаже);

– технологический отдел (каб. 3 на 2-м этаже): изготовление заливного материала из силикон-сырья, настройка оборудования для изготовления форм заливки необходимого размера, производство силиконовых форм согласно заказу, упаковка готового продукта, подготовка товаров к отгрузке сторонней транспортной компанией. В штате – гл. специалист и два инженера 1-й категории;

– служба автоматизации (IT) (каб. 2 на 2-м этаже): сопровождение информационных систем, приобретение и внедрение в организации всех программно-аппаратных средств и средств коммуникаций

(в рамках утвержденных финансового плана и бюджета), обеспечение бесперебойной работы сетевого оборудования, компьютерной техники коллективного пользования, оборудования передачи данных, средств связи, контроль соблюдения сотрудниками организации установленных правил эксплуатации средств вычислительной техники. В штате – системный администратор и инженер технической поддержки 1-й категории;

– отдел кадров (ОК) и организационно-правовой работы (каб. 6 на 3-м этаже): комплектование завода кадрами рабочих и служащих требуемых профессий, разработка, утверждение, осуществление кадровой политики и кадровой стратегии завода и контроль за их соблюдением, ведение кадровой работы, кадрового учета, обеспечение соблюдения трудового законодательства в организации. В штате – начальник отдела, ст. инспектор, юрист по договорно-правовой работе.

Заместителю по экономике (каб. 4 на 3-м этаже) подчиняются:

– бухгалтерия с кассой (каб. 4 на 2-м этаже): ведение достоверного бухгалтерского, налогового и управленческого учета финансово-хозяйственной деятельности завода, формирование и сдача бухгалтерской, налоговой и управленческой отчетности финансово-хозяйственной деятельности завода, взаимодействие с государственными налоговыми и иными органами в пределах своей компетенции, начисление и выплата в установленные сроки заработной платы работникам, осуществление платежей в наличной и безналичной форме в порядке, определяемом внутренними документами завода. В штате – гл. бухгалтер, экономист, бухгалтер, кассир;

– отдел маркетинга (каб. 2 на 3-м этаже): разработка для завода в целом и отдельных товарных групп долгосрочных и текущих планов маркетинга и координация в данной области деятельности подразделений предприятия, оперативное информационное обеспечение маркетинговой деятельности всего предприятия и его подразделений, создание имиджа преуспевающей и надежной фирмы, прием заказов и продажа продукции завода через сайт завода. В штате – начальник отдела (каб. 2 на 3-м этаже), ст. маркетолог-аналитик, маркетолог-аналитик;

– финансово-экономический отдел (каб. 5 на 3-м этаже): эффективное и целевое использование бюджетных средств, разработка проектов, текущих и перспективных финансовых планов, прогнозов бюджетов, экономических расчетов к проекту бюджета, своевременное проведение расчетов с поставщиками и подрядчиками. В штате – начальник отдела (каб. 5 на 3-м этаже), ст. экономист, экономист, инженер 2-й категории.

В подчинении начальнику отдела кадров находятся: водитель – две ставки; слесарь-сантехник – 0,5 ставки, электрик – 0,5 ставки, дворник – 0,5 ставки, уборщица – 0,5 ставки.

Структура СБ и основные задачи структурных подразделений следующие:

– группа охраны и режима: контроль обеспечения охраны объекта со стороны частной охранной организации, контроль работоспособности охранно-тревожной сигнализации (ОТС), системы контроля управления доступом (СКУД) и систем видеонаблюдения (СВН), контроль эксплуатационно-технического обслуживания данных систем, обеспечение контрольно-пропускного и объектового режима (КПиОР), доставка ценных грузов, проверка почтовых сообщений;

– группа режима КИ: контроль ведения конфиденциального делопроизводства, работа с персоналом и посетителями, контроль публикаторской и издательской деятельности, работа со СМИ, контроль обеспечения режима коммерческой тайны (КТ);

– группа ИБ и ТЗИ: администрирование безопасности ЛВС и ЭВМ, реализация защищенных технологий обработки информации, техническая защита от утечки информации по техническим каналам;

– юрисконсульт и аналитик по безопасности: юридическое сопровождение обеспечения безопасности, организационное обеспечение информационной безопасности (ИБ), аналитическая работа.

Таблица 1.1

Общая характеристика штатного персонала объекта (кроме обслуживающего персонала, основных и вспомогательных рабочих)

№ п/п	Структурное подразделение	Расположение (номер кабинета/номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
1	Руководство	1 – 3-й этаж/16	Гендиректор/3	16	Высшее техническое профильное	8	7
2	Руководство	2 – 3-й этаж/18	Зам. по экономике /7	18	Высшее экономическое	7	6
3	Канцелярия	6 – 2-й этаж/14	Зав. канцелярией/4	14, 17, 15	Высшее техническое профильное	8	7
4	Канцелярия	1а – 3-й этаж/17	Секретарь/6	17, 14, 15	Среднее специальное	5	3
5	Канцелярия	7 – 2-й этаж/15	Зав. архивом/13	15, 14	Среднее специальное	5	3
6	Служба безопасности	4 – 3-й этаж/23	Начальник СБ/3	23, 24, 13, 25, 26, 27	Высшее военное	7	7
7	Служба безопасности	4 – 3-й этаж/24	Ст. инспектор СБ/3	24	Высшее техническое профильное	8	8
8	Служба безопасности	6 – 2-й этаж/13	Инспектор группы режима КИ/3	13, 14, 17, 15	Высшее гуманитарное	6	6
9	Служба безопасности	4 – 3-й этаж/25	Администратор безопасности/6	Все (1 – 34)	Высшее техническое профильное	10	9
10	Служба безопасности	5 – 3-й этаж/26	Ст. инспектор СБ (ИБ и ТЗИ)/5	26, 27	Высшее техническое профильное	7	7
11	Служба безопасности	5 – 3-й этаж/27	Инспектор СБ (ИБ и ТЗИ)/4	27, 26	Высшее военное	7	7

Продолжение табл. 1.1

№ п/п	Структурное подразделение	Расположение (номер кабинета/номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
12	Служба безопасности	5 – 3-й этаж/28	Ст. юрисконсульт/5	28, 29	Высшее военное	6	6
13	Служба безопасности	5 – 3-й этаж/29	Аналитик/6	29, 28	Высшее гуманитарное	6	5
14	Технологический отдел	3 – 2-й этаж/5	Главный специалист/3	5, 6, 7	Высшее техническое	7	4
15	Технологический отдел	3 – 2-й этаж/6	Инженер 1-й категории/4	6, 7	Высшее техническое	7	5
16	Технологический отдел	3 – 2-й этаж/7	Инженер 1-й категории/5	7, 6	Высшее техническое профильное	6	5
17	Служба автоматизации (IT)	1 – 2-й этаж/33	Системный администратор/5	Все (1 – 34)	Высшее техническое	9	7
18	Служба автоматизации (IT)	1 – 2-й этаж/34	Инженер технической поддержки 1-й категории/5	Все (1 – 34)	Высшее гуманитарное	9	6
19	Отдел кадров и организационно-правовой работы	6 – 3-й этаж/30	Начальник отдела/4	30, 31, 32	Высшее техническое	5	3
20	Отдел кадров и организационно-правовой работы	6 – 3-й этаж/31	Ст. инспектор ОК/6	31, 32	Высшее техническое	4	3
21	Отдел кадров и правовой работы	6 – 3-й этаж/32	Юрист по договорно-правовой работе/3	32, 31	Высшее юридическое	5	3

Окончание табл. 1.1

№ п/п	Структурное подразделение	Расположение (номер кабинета/номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
22	Бухгалтерия	4 – 2-й этаж/8	Главный бухгалтер/6	8, 9, 10, 11	Высшее экономическое	5	3
23	Бухгалтерия	4 – 2-й этаж/9	Экономист/3	9, 10, 11	Высшее экономическое	4	3
24	Бухгалтерия	4 – 2-й этаж/10	Бухгалтер/5	10, 11	Высшее экономическое	5	4
25	Бухгалтерия	касса – 2-й этаж/11	Кассир/3	11, 10	Среднее специальное	6	5
26	Отдел маркетинга	2 – 3-й этаж/19	Начальник отдела маркетинга/4	19, 20, 21	Высшее экономическое	6	4
27	Отдел маркетинга	2 – 3-й этаж/20	Ст. маркетолог-аналитик/6	20, 21	Высшее экономическое	5	3
28	Отдел маркетинга	2 – 3-й этаж/21	Маркетолог-аналитик/3	21, 20	Среднее специальное	6	5
29	Финансово-экономический отдел	2 – 2-й этаж/1	Начальник финансово-экономического отдела/5	1, 2, 3, 4	Высшее экономическое	4	4
30	Финансово-экономический отдел	2 – 2-й этаж/2	Ст. экономист/7	2, 3, 4	Высшее экономическое	5	3
31	Финансово-экономический отдел	2 – 2-й этаж/3	Экономист/8	3, 4	Высшее экономическое	4	3
32	Финансово-экономический отдел	2 – 2-й этаж/4	Инженер 2-й категории/3	4, 3	Высшее экономическое	3	2

В таблице 1.2 приведена структура защищаемой информации.

Таблица 1.2

Структура защищаемой информации

№ п\п	Наименование источника информации	Гриф конфиденциальности	Источник информации	Место нахождения источника информации
1	Структура предприятия	К	Контракты, документы на бумажных носителях, персонал фирмы	Сейф с документами, каб. 1; ПК 13, 8, 16
2	Личные сведения о сотрудниках фирмы	ПДн	Документы на бумажных и электронных носителях, базы данных (БД), персонал фирмы	Сейф с документами, каб. 1; ПК 13, 14
3	Учредительные документы	К	Устав организации, бумажные документы	Рабочий стол в кабинете директора, секретаря; ПК 16, 17
4	Сведения о кредитах, контрактах	К	Документы на бумажных и электронных носителях, БД, гл. бухгалтер	Рабочий стол в кабинете директора, секретаря, сейф с документами, каб. 1; ПК 16, 17, 8, 18
5	База данных заказчиков, партнеров фирмы	КТ	Документы на бумажных и электронных носителях, гл. бухгалтер	Рабочий стол в кабинете директора, секретаря, сейф с документами, каб. 1; ПК 16, 17, 8, 18
6	Сведения о конкурентах (в том числе компромат)	КТ	Документы на бумажных и электронных носителях	Сейф с документами, каб. 1; ПК 16, 18
7	Сведения о распределении прибыли между сотрудниками	К	Документы на бумажных и электронных носителях, гл. бухгалтер	Сейф с документами, каб. 1; ПК 16, 18
8	Пароли к используемому ПО и web-сайтам	КТ	Документы на электронных носителях, СБ, отдел IT	ПК 25, 33
9	Архив названий, логотипов, рекламных буклетов и роликов фирм-заказчиков	СК	Документы на бумажных и электронных носителях, отдел маркетинга	Сейф с документами, каб. 1; ПК 25, 33, 28

Окончание табл. 1.2

№ п\п	Наименование источника информации	Гриф конфиденциальности	Источник информации	Место нахождения источника информации
10	Сведения о концепте и продвижении продукции	КТ	Документы на бумажных и электронных носителях, отдел маркетинга	Сейф с документами, каб. 1; ПК 16, 18
11	Методы и способы производства, новые технологии	КТ	Документы на бумажных и электронных носителях, отдел маркетинга	Сейф с документами, каб. 1; ПК 16, 18
12	Конкурентоспособность производимой продукции, эффективность экспорта и импорта	СК	Документы на бумажных и электронных носителях, отдел маркетинга	Сейф с документами, каб. 1; ПК 16, 18
13	Планы и характер рекламной и публикаторской деятельности	КТ	Документы на бумажных и электронных носителях, юрисконсульты	Сейф с документами, каб. 1; ПК 16, 28
14	Сведения о системе безопасности организации	КТ	Документы на бумажных и электронных носителях, СБ, рабочий стол директора	Сейф с документами, каб. 1; ПК 13, 14
15	Телефонные переговоры сотрудников и клиентов	КТ	Документы на электронных носителях, СБ, отдел IT	ПК 23, 24, 26
16	Направления модернизации известных технологий	КТ	Документы на бумажных и электронных носителях, отдел маркетинга	Сейф с документами, каб. 1; ПК 16, 19
17	Изобретения и полезные модели, используемые инновации и ноу-хау производства	КТ	Документы на бумажных и электронных носителях, отдел маркетинга	Сейф с документами, каб. 1; ПК 33, 34

Генплан расположения объекта на местности приведен на рис. 1.2.

Рис. 1.2. Генплан расположения объекта на местности

Поэтажные планы расположения по помещениям средств вычислительной техники (СВТ) представлены на рис. 1.3.

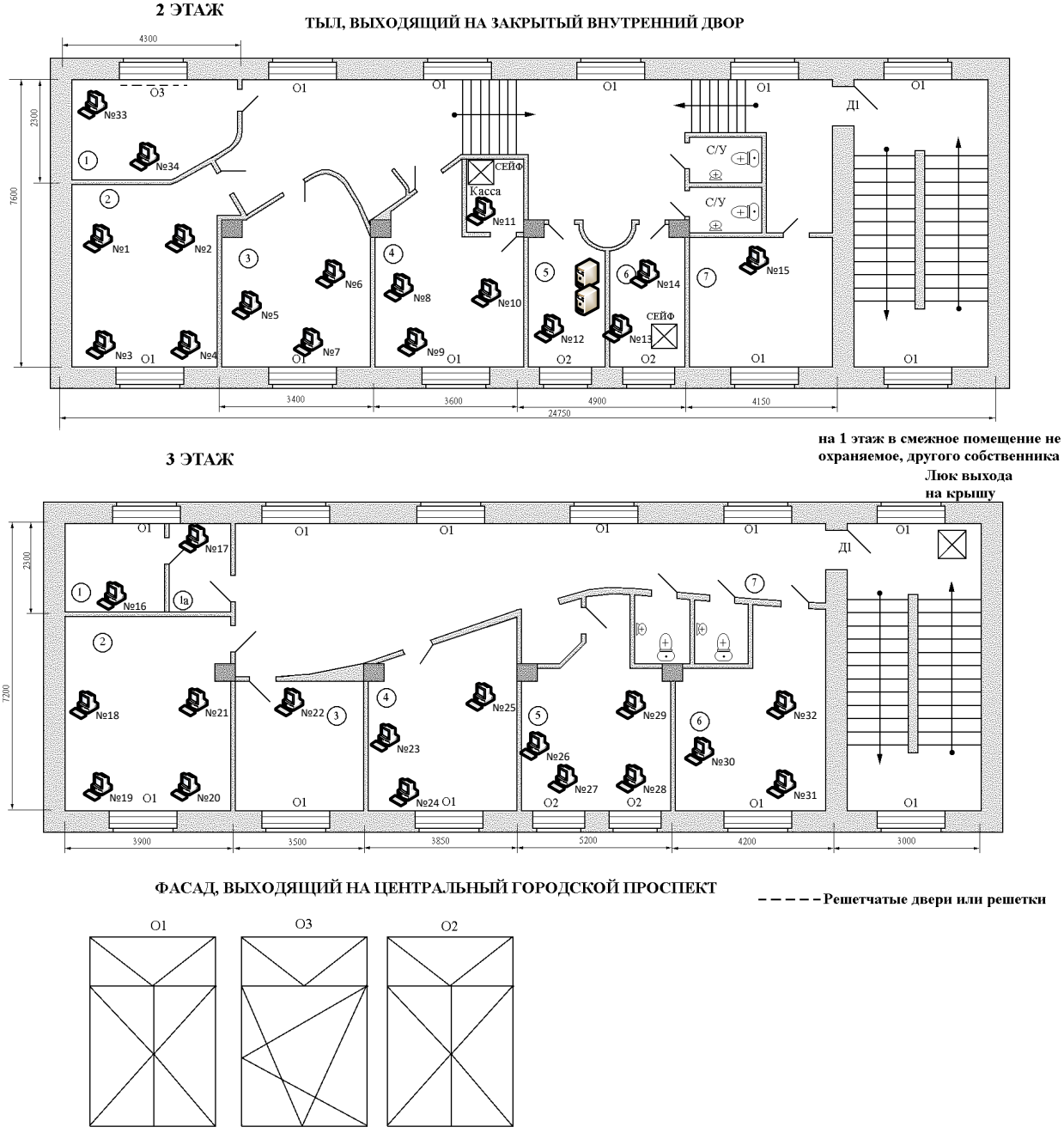

Рис. 1.3. Поэтажные планы расположения СВТ

Пример пояснительной записки с обоснованием выбора топологии ЛВС приведен ниже.

На ООО «Пример» будет использоваться топология «звезда», так как отказы в работе на отдельных участках сети не влияют на работо-

способность остальной части. Эта топология наиболее надежна. Упрощен поиск неисправностей сети, активные концентраторы часто наделены диагностическими возможностями, позволяющими определить работоспособность соединения. Следовательно, работу сети такой топологии легче восстановить после сбоев, чем другие.

Решающие факторы при выборе – следующие особенности топологии «звезда»: к каждому узлу будет проложен отдельный сетевой кабель, что позволит расположить рабочие станции произвольным образом. Разрыв одного из кабелей может сказаться лишь на работоспособности одного узла и быть быстро локализован.

В качестве центрального узла «звезды» будет использоваться надежное оборудование – коммутатор («switch») одного из лидирующих производителей, что обеспечит высокую отказоустойчивость сети в целом. С центрального узла можно будет контролировать состояние подключения всех остальных узлов благодаря тому, что концентратор имеет специальные индикаторы подключения и состояния подключения для каждого узла. Преимущества – гибкость, возможность расширения, относительно низкая стоимость развертывания по сравнению с более сложными топологиями локальных сетей со строгими методами доступа к среде передачи данных.

Пример пояснительной записки с обоснованием выбора пассивного и активного сетевого оборудования приведен ниже.

Для структурированных кабельных систем (СКС) используют специальное оборудование, которое можно разделить на два основных типа – активное и пассивное.

Выбор пассивного оборудования ЛВС

Пассивное оборудование не потребляет электроэнергию и не передает сигналы. Оно включает в себя различные проводники, розетки, кабели, коннекторы, монтажные шкафы, коммуникационные панели, кроссы, стойки, кабельные каналы, патч-корды и др.

В проектируемой СКС был выбран одножильный медный кабель «витая пара» категории 5е производства Cabeus.

На ООО «Пример» для укладки кабеля при монтаже были выбраны короба 40×25П DeGross. В проектируемой СКС были выбраны двойные внутренние розетки RJ45 категории 5е Scneider sdN4400147.

Коннекторы монтируются обжимным способом на концах патч-кордов. Коннектор RJ45 – стандарт витой пары (UTP).

На ООО «Пример» были выбраны коммутационные шнуры UTP, отвечающие требованиям категории 5e, имеющие на концах коннекторы типа RJ45 производства Exalan+.

На ООО «Пример» предусмотрены организация серверной комнаты (пом. 5 на 2-м этаже) и использование серверного оборудования. Рационально сделать выбор в пользу монтажной стойки. Была выбрана 19-дюймовая монтажная стойка 45 U высотой 2,20 м AESP REC-45UB-GY.

Для размещения серверов был выбран напольный 19-дюймовый шкаф со стеклянной дверью, высота которого равна 22 U, AESP REC-6226S SignaPro 224. Размеры шкафа 600×600×1165 мм.

Для размещения коммутаторов на 3-м этаже головного офиса и в технологическом отделе используются телекоммуникационные настенные шкафы ШРН-6.300, 6 U (600×300 мм), дверь – стекло. Также необходимо использовать такое пассивное оборудование, как гофрированные шланги для монтажа под потолком, труба ПВХ для соединения между этажами, и некоторые сопутствующие детали и аксессуары для пассивного оборудования.

Выбор активного оборудования ЛВС

Активное оборудование охватывает коммутаторы ядра, доступа, распределения, маршрутизаторы, трансиверы, серверы, сетевые адаптеры, репитеры и другие устройства. Любое активное оборудование потребляет электроэнергию и передает сигналы. Поэтому для надежной работы требуется источник бесперебойного питания.

На ООО «Пример» используется такое активное оборудование, как коммутаторы и серверы. Рабочие станции должны быть оснащены сетевыми адаптерами для возможности подключения к ЛВС.

Все активное оборудование будет установлено в коммутационный шкаф и монтажную стойку. Выбраны следующие коммутаторы:

– D-link DES-1008D (коммутатор с восемью портами 10/100 Мбит/с, скорость передачи данных Fast Ethernet – до 200 Мбит/с);

– D-link DES-1026G (коммутатор с 24 портами 10/100Base-TX и двумя комбопортами 100/1000Base-T/SFP, скорость передачи данных Fast Ethernet – до 200 Мбит/с).

Определение протокола передачи данных

Для проектируемой ЛВС будет использоваться стек протоколов TCP/IP. Он наиболее универсален и подходит для интеграции распределенных сетей филиалов. TCP/IP будет использоваться в локальных сетях офисов. В этом случае весь потенциал этого стека протоколов не будет задействован, стек будет использоваться как наиболее распространенное и хорошо известное решение.

Преимущества TCP/IP реализуются при интеграции сетей филиалов. Это достигается благодаря одному из основных протоколов стека – TCP – на транспортном уровне. Этот протокол определяет способ для двух удаленных узлов проверить, все ли данные были переданы, не потеряли ли данные целостности, и при необходимости позволяет повторную передачу данных.

Разделение сети на подсети

При логической структуризации сети необходимо решить проблему перераспределения передаваемого трафика между различными физическими сегментами сети.

Локальная вычислительная сеть ООО «Пример» будет состоять из двух сетей: сети головного офиса и сети технологического отдела. Каждая сеть будет использовать протокол Fast Ethernet на базе собственного коммутатора. Всего их три (два – на двух этажах головного офиса (по одному на этаж) и один – в технологическом отделе).

Логическая структура сети представлена в файле «Структурная схема ЛВС с указанием ip.vsd».

Выбор сетевой технологии

Локальные сетевые технологии, наиболее часто используемые при проектировании ЛВС, – Ethernet, Token Ring, FDDI. В ООО «Пример» выбрана наиболее эффективная по соотношению цена/качество и обеспечивающая надежность передачи данных и производительность до 200 Мбит/с технология Fast Ethernet. Для горизонтальной кабельной системы наиболее предпочтительная среда передачи данных – витая пара, поскольку данный тип кабеля удовлетворяет требованиям гибкости, удобства его прокладки в помещениях, простоты монтажа, имеет среднюю стоимость.

В качестве физического интерфейса был выбран 100Base-TX.

Пример распределения ПК по коммутаторам представлен в табл. 1.3.

Таблица 1.3

Распределение ПК по коммутаторам

Номер этажа	Номер кабинета	Структурное подразделение	Наименование кабинета	Номера ПК, установленных в кабинете
Коммутатор 1 (2-й этаж)				
2	Касса	Бухгалтерия	Кассир	11
2	1	Служба автоматизации (IT)	Системный администратор	33
2	1	Служба автоматизации (IT)	Инженер технической поддержки 1-й категории	34
2	2	Финансово-экономический отдел	Начальник финансово-экономического отдела	1
2	2	Финансово-экономический отдел	Ст. экономист	2
2	2	Финансово-экономический отдел	Экономист	3
2	2	Финансово-экономический отдел	Инженер 2-й категории	4
2	4	Бухгалтерия	Гл. бухгалтер	8
2	4	Бухгалтерия	Экономист	9
2	4	Бухгалтерия	Бухгалтер	10
2	6	Канцелярия	Зав. канцелярией	14
2	6	Служба безопасности	Инспектор группы режима КИ	13
2	7	Канцелярия	Зав. архивом	15
Коммутатор 2 (3-й этаж)				
3	1	Руководство	Ген. директор	16
3	1а	Канцелярия	Секретарь	17
3	2	Руководство	Зам. по экономике	18
3	2	Отдел маркетинга	Начальник отдела маркетинга	19
3	2	Отдел маркетинга	Ст. маркетолог-аналитик	20
3	2	Отдел маркетинга	Маркетолог-аналитик	21
3	4	Служба безопасности	Начальник СБ	23
3	4	Служба безопасности	Ст. инспектор СБ	24
3	4	Служба безопасности	Администратор безопасности	25
3	5	Служба безопасности	Ст. инспектор СБ (ИБ и ТЗИ)	26

Окончание табл. 1.3

Номер этажа	Номер кабинета	Структурное подразделение	Наименование кабинета	Номера ПК, установленных в кабинете
3	5	Служба безопасности	Инспектор СБ (ИБ и ТЗИ)	27
3	5	Служба безопасности	Ст. юрисконсульт	28
3	5	Служба безопасности	Аналитик	29
3	6	Отдел кадров и организационно-правовой работы	Начальник отдела	30
3	6	Отдел кадров и организационно-правовой работы	Ст. инспектор ОК	31
3	6	Отдел кадров и организационно-правовой работы	Юрист по договорно-правовой работе	32
Коммутатор 3 (2-й этаж)				
2	3	Техническая группа	Главный специалист	5
2	3	Техническая группа	Инженер 1-й категории	6
2	3	Техническая группа	Инженер 1-й категории	7

Расчет длины кабеля

Горизонтальная подсистема обеспечивает соединение рабочих мест с кроссовым оборудованием. Выполнена четырехпарным одножильным медным кабелем «витая пара» категории 5е. Сопротивление (100 ± 15) Ом. Емкость 4,59 нФ/100 м на частоте 1 кГц.

Требуемое количество кабеля от коммутатора до автоматизированного рабочего места (АРМ) рассчитывается с использованием следующего эмпирического метода. Исходя из предположения, что рабочие места распределены по обслуживаемой площади равномерно, вычисляется *средняя длина кабельных трасс* по формуле $L_{ср} = (L_{max} + L_{min})/2$, где L_{min} и L_{max} – соответственно длина кабельной трассы от точки размещения коммутатора до информационного разъема самого близкого и самого далекого рабочего места, посчитанная с учетом технологии прокладки кабеля, всех спусков, подъемов, поворотов и особенностей здания. При определении длины трасс необходимо учесть технологический запас 10 % от $L_{ср}$ и запас X (примем X = 2 м)

для процедур разводки кабеля в распределительном узле и информационном разъеме. Далее прибавляем длину кабеля $L_{ком}$ от сервера до коммутатора.

Таким образом, *длина трасс* составит

$L = (1{,}1L_{ср} + X)N + L_{ком}$,

где N – количество розеток. В формуле берем $2N$, так как на рабочих местах должны устанавливаться две информационные розетки RJ45.

Головной офис, 2-й этаж

$L_{ком1} = 2$ м; $L_{max} = 20{,}95$ м; $L_{min} = 2{,}45$ м; $L_{ср} = 11{,}7$ м;

$L_{го2} = (1{,}1 \cdot 11{,}7 + 2)12 \cdot 2 + 2 = 358{,}88$ м

Головной офис, 3-й этаж

$L_{ком2} = 3$ м; $L_{max} = 25{,}25$ м; $L_{min} = 1$ м; $L_{ср} = 13{,}13$ м;

$L_{го3} = (1{,}1 \cdot 13{,}13 + 2)16 \cdot 2 + 3 = 529{,}18$ м

Технологический отдел

$L_{ком3} = 61{,}5$ м; $L_{max} = 8{,}7$ м; $L_{min} = 0{,}5$ м; $L_{ср} = 4{,}6$ м;

$L_{то} = (1{,}1 \cdot 4{,}6 + 2)3 \cdot 2 + 61{,}5$ м $= 103{,}86$ м

$L = L_{го2} + L_{го3} + L_{то} = 991{,}9$ м.

Длина кабель-канала

$L_к = 0{,}75\ L = 743{,}9$ м.

Максимально возможное расстояние от рабочих станций до коммутаторов в сети для кабелей категории 5е составляет не более 90 м. В данных расчетах видно, что максимальная длина кабеля не превышает 90 м – наибольшей длины для четырехпарного одножильного медного кабеля «витая пара» категории 5е.

Выбор оборудования и аппаратно-программной конфигурации

Выбор ПО. На рынке операционных систем представлено несколько линеек сетевых операционных систем от разных фирм-разработчиков. При выборе сетевой операционной системы для планируемой ЛВС необходимо иметь в виду средний уровень пользования ПК работниками. В связи с этим была выбрана наиболее популярная и знакомая рядовому пользователю операционная система Windows 10.

В качестве серверной операционной системы будем использовать Windows 2012 Server, поскольку она предлагает большие возможности по управлению доменами, пользователями, группами и безопасности.

Будут использоваться следующие возможности серверной операционной системы: поддержка стека протоколов TCP/IP; служба сервера домена (Active Directory); служба трансляции сетевых адресов (Network Address Translation (NAT)).

Для рабочих станций будет использоваться Windows 10 и следующие ее возможности: поддержка стека протоколов TCP/IP; графический интерфейс пользователя.

Восстановление системы. При сбое компьютер переходит в Safe Mode (безопасный режим), операционная система предлагает возможность отката System Restore (восстановление системы). Это позволяет пользователю вернуться к тем установкам, которые имелись на компьютере до инцидента. Так называемые точки восстановления (restore points) могут быть созданы пользователем в любое время. Кроме того, операционная система периодически создает свои точки восстановления при каждой инсталляции новой программы. При откате компьютера к точке восстановления операционная система использует установочные данные, соответствующие тому времени, когда система работала нормально.

В качестве офисного пакета был выбран бесплатный профессиональный офисный пакет программ LibreOffice. В его состав входят следующие компоненты: Writer, Calc, Impress, Draw, Base, Math, а также средство для создания файлов в формате PDF.

Для обеспечения работы отделов ООО «Пример» используются пакеты семейства 1С: 1С:Бухгалтерия, 1С:Зарплата, 1С:Кадры, 1С:Склад, поддержка которых осуществляется силами службы автоматизации IT.

Организация безопасной работы ЛВС невозможна без применения антивирусного программного обеспечения. В качестве антивирусной защиты была выбрана надежная отечественная система Kaspersky Endpoint Security 11 для Windows. Kaspersky Endpoint Security 11 включает в себя многоуровневую защиту от угроз, проактивные технологии

(контроль программ и устройств, веб-контроль), средства управления уязвимостями и установкой исправлений, а также шифрование данных.

Выбор аппаратного обеспечения

Выбранная модель коммутатора для сети технологического отдела – D-link DES-1008D (коммутатор с восемью портами 10/100 Мбит/с, скорость передачи данных Fast Ethernet – до 200 Мбит/с).

Выбранная модель коммутаторов для головного офиса – D-link DES-1026G (коммутатор с 24 портами 10/100Base-TX и двумя комбопортами 100/1000Base-T/SFP, скорость передачи данных Fast Ethernet – до 200 Мбит/с).

Разработка спецификаций на сеть

На серверах ООО «Пример» устанавливается операционная система Windows 2012 Server. На рабочих станциях устанавливается операционная система Microsoft Windows 10. Общее программное обеспечение включает в себя пакет LibreOffice.

Автоматизированные рабочие места работников головного офиса будут объединены в общую сеть, АРМ технологического отдела – в отдельную сеть, не связанную с головным офисом. Каждая рабочая станция головного офиса будет иметь доступ в Интернет. В качестве маршрутизатора будет использоваться сервер головного офиса.

В проектируемой сети не будет использоваться протокол DHCP, который позволяет динамически назначать адреса для рабочих станций. Адреса будут настроены вручную. В каждой сети АРМ будет назначен IP-адрес 192.168.x.y. Рабочие станции головного офиса будут иметь адреса 192.168.0.y, где y – номер компьютера. Рабочие станции технологического отдела будут иметь адреса 192.168.1.y, где y – номер компьютера. Таким образом, каждый узел будет иметь свой уникальный адрес, а значит, может быть адресован в пределах сети. Такая адресация называется «серой», так как указанные IP-адреса не могут быть адресованы из Интернета, именно для этого на сервере для доступа к Интернету будет использоваться служба NAT. Соответственно, у сервера будет исходящий «белый» IP-адрес, какой именно – назначит провайдер Интернета.

В рамках этой оценки для ПО MSAT были предоставлены следующие ответы (табл. 1.4).

Таблица 1.4

Оценка ПО MSAT

Вопрос оценки	Ваш ответ
Business Risk Profile	
Число используемых настольных и переносных компьютеров в компании	Менее 50
Число используемых серверов в компании	1 – 5
Используется ли в вашей компании постоянное подключение к Интернету?	Да
Получают ли клиенты и поставщики доступ к сети или внутренним системам по Интернету?	Нет
Предоставляет ли ваша компания на своем узле такие службы приложений, как портал или веб-узел, для внешних клиентов или партнеров?	Да
Развертывает ли ваша организация службы, используемые как внешними, так и внутренними клиентами в одном и том же сегменте?	Да
Подключаются ли внешние партнеры или клиенты непосредственно к внутренним серверным системам компании с целью получения доступа к данным, записи обновлений или обработки информации?	Нет
Развертывала ли ваша организация идентичные компоненты серверной инфраструктуры, например базы данных, для поддержки как внешних приложений, так и внутренних корпоративных служб?	Нет
Разрешено ли сотрудникам или подрядчикам вашей организации пользоваться удаленным доступом для подключения к внутренней корпоративной сети?	Нет
Разрешено ли сотрудникам в вашей организации развертывать непроизводственные системы, например личные веб-серверы или компьютеры, на которых хранятся «любимые проекты», в общей корпоративной сети?	Нет
Разрешена ли в вашей организации, помимо резервных носителей/ленточных носителей, обработка конфиденциальных или принадлежащих компании данных за пределами сети?	Нет

Продолжение табл. 1.4

Вопрос оценки	Ваш ответ
Сильно ли повлияет дискредитация безопасности систем в вашей среде на способность компании вести дела?	Нет
Пользуется ли ваша компания офисным пространством совместно с другими организациями?	Нет
Разрабатывает ли ваша компания приложения?	Нет
Разрешено ли разработчикам программного обеспечения в вашей организации пользоваться удаленным доступом для подключения к корпоративным ресурсам, связанным с разработкой, или удаленно разрабатывать код приложения?	Нет
Разрабатывает ли ваша компания и поставляет ли программные продукты клиентам, партнерам или на рынок широкого потребления?	Нет
Разрешено ли разработчикам в вашей организации вести разработку или тестировать системы удаленно или в каких-либо местах в незащищенных условиях?	Нет
Выступает ли ваш персонал ИТ в роли хранителя (в отличие от разработчика) важных бизнес-приложений?	Нет
Требуется ли использовать в бизнес-процессах данные, которые хранятся, обрабатываются или распределяются третьей стороной?	Нет
Хранит или обрабатывает ваша компания данные клиента в общей среде совместно с корпоративными ресурсами?	Нет
Полагаетесь ли вы на сторонних партнеров по разработке программных продуктов с целью поддержки предложений, связанных с бизнес-службами?	Нет
Получает ли ваша компания доход от предложения услуг, требующих обработки данных или информационной проходки?	Нет
Считает ли ваша организация данные, обработанные службами приложений компании, конфиденциальными или важными для деловых операций клиентов?	Нет

Продолжение табл. 1.4

Вопрос оценки	Ваш ответ
Доступны ли основные бизнес-приложения компании через интернет-соединения?	Нет
Кто является целевыми пользователями основных приложений в вашей среде?	Внутренние сотрудники
Каким образом основные приложения становятся доступны пользователям?	Только из внутренней сети
Подключена ли корпоративная сеть к сетям клиента, партнера или сторонним сетям по сетевым соединениям – общедоступным или частным?	Нет
Получает ли ваша компания доход от услуг, в основе которых лежит хранение или распределение данных в электронном виде, например файлов мультимедиа или документации?	Нет
Прошла ли ваша организация через изменение «копирование и замена», касающееся любого основного компонента технологии, за последние шесть месяцев?	Нет
Полагается ли ваша компания на данные, полученные от партнеров, поставщиков или из сторонних источников или обработанные ими?	Нет
Повлияет ли на доходность событие, нанесшее вред приложениям или инфраструктуре клиента, например бездействие узла, отказ оборудования или сбой в приложении?	Да
Хранит ли ваша компания конфиденциальные или важные данные клиентов?	Да
Зависит ли работа компонентов или приложений инфраструктуры клиентов от доступа к ресурсам в вашей среде?	Нет
Используются ли инфраструктура и компоненты приложений вашей компании несколькими клиентами?	Нет
Развертывает ли ваша организация новые службы или приложения до выполнения их оценки, относящейся к возможным проблемам безопасности?	Нет
Регулярно ли ваша организация меняет учетные данные для привилегированных учетных записей?	Да

Продолжение табл. 1.4

Вопрос оценки	Ваш ответ
Меняет ли ваша организация учетные данные для привилегированных учетных записей после увольнения персонала с привилегированным доступом?	Да
Считаете ли вы, что информационные технологии являются необходимым условием для вашей компании?	Нет
Все ли сотрудники в вашей компании используют компьютеры для бизнеса?	Нет
Привлекает ли ваша компания внешний ресурс, управляющий или владеющий любой частью инфраструктуры?	Нет
Существует ли у вашей компании среднесрочный или долгосрочный план для выбора и развертывания компонентов новых технологий?	Да
Считаете ли вы, что ваша организация является ранним последователем в новых технологиях?	Нет
Выбирает и разворачивает ли ваша организация новые технологии на основе существующих партнерских или лицензионных соглашений?	Нет
Ограничивается ли ваша организация в выборе технологий только теми технологиями, которые известны текущему ИТ-персоналу?	Да
Расширяет ли ваша компания свою сеть посредством приобретения новых компаний и существующих в них сред?	Нет
Разрешено ли сотрудникам в вашей организации загружать конфиденциальные данные клиентов или корпоративные данные на свои рабочие станции?	Нет
Ограничивает ли ваша организация доступ пользователей к данным в зависимости от их роли в компании?	Да
Выберите вариант, который наиболее точно описывает отраслевой сегмент вашей компании	Производство (отдельное)
Выберите размер организации	10 – 49 сотрудников
Располагается ли ваша компания в разных местах?	Нет

Продолжение табл. 1.4

Вопрос оценки	Ваш ответ
Относится ли деятельность вашей компании к чрезвычайно конкурентной или сосредоточенной на исследованиях отрасли, в которой кража интеллектуальной собственности или шпионаж может стать серьезной проблемой?	Нет
Существует ли в вашей компании высокая текучесть среди специалистов по технологиям, а также изнурительные условия работы?	Нет
Обладает ли ваша компания продуктом, имеющим важное значение, или широко известной торговой маркой?	Нет
Используется ли в вашей компании программное обеспечение самых ранних версий (которое уже не поддерживается поставщиком)?	Нет
Приобретает ли ваша организация программное обеспечение у известных и надежных поставщиков или источников?	Да
Инфраструктура	
Используются ли в вашей организации на границах сети межсетевые экраны или другие элементы управления доступом на сетевом уровне для защиты корпоративных ресурсов?	Да
Развертывает ли ваша организация эти элементы управления в каждом офисе?	Да
Использует ли ваша организация нейтральную зону (также широко известную как демилитаризованная зона (ДМЗ)), отделяющую внутренние и внешние сети, в которых размещены службы?	Да
Размещены ли в вашей организации службы, связанные с Интернетом?	Да
Используется ли в вашей организации программное обеспечение межсетевого экрана на хост-компьютере для защиты серверов?	Да
Используется ли в вашей организации оборудование или программное обеспечение для определения вторжения, помогающее выявить злонамеренные атаки?	Да

Продолжение табл. 1.4

Вопрос оценки	Ваш ответ
Выберите тип(ы) используемой системы определения вторжения (IDS)	Сетевая система определения вторжения (NIDS)
Реализованы ли в среде антивирусные решения?	Да
Выберите системы, в которых развернуты антивирусные решения	Почтовые серверы Шлюзы доступа (шлюзы, прокси-серверы, ретрансляторы и т. п.) Настольные компьютеры Серверы
Возможен ли удаленный доступ к сети компании?	Нет
Существует ли в сети более одного сегмента?	Да
Используется ли сегментация сети для отделения внешнего клиента и служб внешней сети от корпоративных ресурсов?	Нет
Существует ли возможность беспроводного подключения к сети?	Нет
Существуют ли средства контроля для применения политик паролей к учетным записям разного типа?	Да
Выберите учетные записи, для которых существуют средства контроля для применения политик паролей	Администратор Пользователь
Укажите вариант проверки подлинности, используемый для административного доступа к управлению устройствами и хост-компьютерами	Многофакторная проверка подлинности
Укажите вариант проверки подлинности, используемый для доступа внутренних пользователей к внутренней сети и хост-компьютеру	Сложный пароль
Укажите вариант проверки подлинности, используемый для удаленного доступа пользователей	Нет
Разрешена ли блокировка учетной записи для блокирования доступа после определенного числа неудачных попыток входа в систему?	Да
Разработаны ли в организации процессы наблюдения за неактивными учетными записями администраторов, сотрудников, поставщиков и удаленных пользователей?	Да

Продолжение табл. 1.4

Вопрос оценки	Ваш ответ
Конфигурирование систем выполняется самой компанией или поставщиком оборудования/продавцом?	Конфигурируется внутренним персоналом
Что из приведенного создается на основе образа или формальной документированной конфигурации?	Рабочие станции и переносные компьютеры
Включает ли в себя эта конфигурация процедуры укрепления узла?	Да
Какие из приведенных решений были установлены на рабочих станциях и переносных компьютерах сотрудников?	Экранная заставка с парольной защитой
Разработаны ли в организации формальные процедуры реагирования на нарушения безопасности?	Да
Разработаны ли в организации политики и процедуры создания отчетов в случаях нарушения безопасности или возникновения проблем, имеющих отношение к безопасности?	Да
Развернуты ли элементы управления физической безопасностью для защиты имущества компании?	Да
Какие из приведенных элементов управления безопасностью используются?	Система сигнализации, установленная для обнаружения незаконного вторжения и оповещения Сетевое оборудование (коммутаторы, кабельные системы, интернет-соединение) находится в закрытом помещении с ограниченным доступом Сетевое оборудование находится также в запираемом шкафу/стойке

Продолжение табл. 1.4

Вопрос оценки	Ваш ответ
Какие из приведенных элементов управления безопасностью используются?	Серверы находятся в закрытом помещении с ограниченным доступом Серверы находятся также в запираемых шкафах/стойках Конфиденциальные печатные материалы хранятся в запираемых картотечных шкафах
Какие из перечисленных мер контроля физического доступа используются?	Идентификационные карточки для сотрудников и посетителей Журналы регистрации посетителей Контрольно-пропускные пункты
Приложения	
Существуют ли в вашей компании важные бизнес-приложения (LOB)?	Нет
Используются ли у вас специально разработанные макросы для офисных приложений (например, для Word, Excel или Access)?	Нет
Какие механизмы действуют на местах для обеспечения высокой доступности приложений? Выберите в приведенном списке все развернутые механизмы	Регулярная проверка приложения и восстановление данных
Собственная группа разрабатывала какие-либо основные приложения, развернутые в вашей среде?	Нет
Были ли какие-либо из основных приложений, развернутых в инфраструктуре предприятия, разработаны сторонними консультантами или поставщиками?	Да
Предоставляет ли сторонний консультант или поставщик регулярное обновление программного обеспечения, исправления для системы безопасности и сведения о способах обеспечения безопасности? (Действует ли такая поддержка в настоящее время?)	Проектирование Написание кода Тестирование/контроль качества Окончательная проверка

Продолжение табл. 1.4

Вопрос оценки	Ваш ответ
Регулярно ли сторонний поставщик предоставляет программные обновления и исправления, повышающие безопасность, а также документацию по механизмам безопасности? (Существует ли еще поддержка?)	Нет
Какие методологии разработки систем безопасности программного обеспечения применяются в компании? (Отметьте все подходящие варианты)	Нет
Располагает ли ваша организация сведениями о проблемах безопасности, существующих в каком-либо приложении, используемом в среде?	Нет
Проводит ли компания обучение в области безопасности для разработчиков и испытателей?	Нет
Применяет ли компания программные средства в качестве инструмента тестирования и аудита при разработке защищенного программного обеспечения?	Нет
Существуют ли средства контроля для применения политик паролей в основных приложениях?	Да
Выберите элементы управления, предусматривающие наличие паролей и применяемые для основных приложений	Сложные пароли Истечение срока действия пароля Блокировка учетной записи
Выберите в приведенном списке наиболее распространенный метод проверки подлинности, используемый для основных приложений	Сложный пароль
Существуют ли механизмы для основных приложений в вашей среде, позволяющие ограничивать доступ к критическим данным и функциональным возможностям?	Да
Записываются ли сообщения основных приложений в вашей среде в файлы журналов для проведения анализа и проверки?	Да
Выберите тип регистрируемых событий	Неудачные попытки проверки подлинности Отказ в доступе к ресурсам Изменения в данных Изменения в учетных записях пользователей

Продолжение табл. 1.4

Вопрос оценки	Ваш ответ
Проверяются ли входные данные развернутыми приложениями?	Не знаю
Шифруются ли основными приложениями обрабатываемые ими конфиденциальные и важные данные для бизнеса?	Не знаю
Операции	
Управление средой осуществляется самой компанией или внешним ресурсом?	Средой управляет компания
Используются ли в организации выделенные узлы управления для безопасного управления системами и устройствами в вашей среде?	Да
Выберите системы, для которых существуют выделенные узлы управления	Сетевые устройства Серверы
Используются ли учетные записи для отдельного входа в систему в обычной или административной/управленческой деятельности?	Да
Предоставляет ли организация пользователям административные права доступа к их рабочим станциям и переносным компьютерам?	Нет
Регулярно ли тестируется межсетевой экран в целях обеспечения ожидаемой производительности?	Нет
Разработаны ли в организации планы аварийного восстановления и возобновления деятельности предприятия?	Да
Проходят ли эти планы регулярное тестирование?	Нет
Существует ли модель для назначения уровней критичности каждому компоненту вычислительной среды?	Да
Существуют ли политики для управления вычислительной средой?	Да
Существует ли политика безопасности информации, направленная на регулирование деятельности организации, связанной с безопасностью?	Да
Выберите тех, кто разрабатывал политику	Исключительно отдел ИТ
Существует ли корпоративная политика правильного использования?	Да
Существуют ли политики для управления учетными записями отдельных пользователей?	Да

Продолжение табл. 1.4

Вопрос оценки	Ваш ответ
Выберите из приведенных политик те, что применяются для управления учетными записями отдельных пользователей	Индивидуальные учетные записи пользователей (общие учетные записи отсутствуют) Привилегированные и непривилегированные учетные записи для администраторов Учетные записи уволившихся сотрудников блокируются
Существует ли документированный процесс для сборок хост-компьютеров? Если да, то укажите, какого типа (Для каких типов хост-компьютеров существует документированный процесс для сборок?)	Нет
Существуют ли документированные указания, которые предписывают, какие протоколы и службы разрешены в корпоративной сети? Выберите используемый вариант	Указания существуют и документированы
Разработана ли в организации формальная и документально оформленная процедура утилизации данных на электронных и бумажных носителях?	Да
Разработана ли в компании схема классификации данных с соответствующими рекомендациями по их защите?	Да
Существует ли процесс управления изменениями и конфигурацией?	Нет
Существует ли установленная политика исправлений и обновлений, а также сам процесс?	Да
Выберите компоненты, для которых они существуют	Операционные системы и приложения
Проверяет ли организация исправления и обновления до их развертывания?	Да
Укажите, что из приведенного используется для развертывания исправлений и управления ими	Windows Server Update Services (WSUS)
На хост-компьютерах какого типа используется автоматизированное управление исправлениями?	Рабочие станции и переносные компьютеры Серверы

Продолжение табл. 1.4

Вопрос оценки	Ваш ответ
Существует ли установленная политика, направленная на обновление продуктов обнаружения по сигнатуре?	Антивирус
Существуют ли точные логические схемы и справочная документация по конфигурации для сетевой инфраструктуры и хост-компьютеров?	Нет
Существуют ли точные схемы архитектуры приложений и потоков данных для основных приложений?	Нет
Ведутся ли журналы в среде для записи событий на хост-компьютерах и устройствах?	Нет
Регулярно ли резервируются важные и критические данные?	Да
Существуют ли политики и процедуры для хранения резервных носителей и работы с ними?	Да
Какие из приведенных политик и процедур применяются	Хранение в запираемых несгораемых корпусах Ограниченный доступ персонала к резервным носителям Ротация и жизненный цикл резервных носителей
Существуют ли политики для регулярной проверки процедур архивации и восстановления? Документированы ли эти политики?	Да, они документированы
Персонал	
Существует ли в вашей компании в отношении безопасности индивидуальная или групповая ответственность?	Да
Обладает ли такое лицо или группа должным опытом в области безопасности?	Да
Участвует ли это лицо или группа в определении требований по безопасности для новых и существующих технологий?	Да
На каких стадиях жизненного цикла технологий привлекается данная группа или лицо, обеспечивающее безопасность?	Планирование и проектирование Реализация Тестирование Развертывание

Окончание табл. 1.4

Вопрос оценки	Ваш ответ
Определены ли роли и обязанности для каждого лица, связанного с информационной безопасностью?	Да
Используются ли независимые сторонние специалисты для организации оценки безопасности среды?	Нет
Выполняют ли оценку безопасности среды внутренние специалисты организации?	Да
С какой периодичностью выполняется такая оценка безопасности?	Ежегодно
Выберите области анализа, которые охватываются этой оценкой	Инфраструктура Политика Проверка
Выполняются ли в организации проверки в фоновом режиме, являющиеся составной частью процесса найма?	Нет
Существует ли официальная политика в отношении служащих, покидающих компанию?	Да
Выберите варианты, в которых существует официальная политика в отношении служащих, покидающих компанию	Конфликтные увольнения Увольнения по соглашению сторон
Существует ли официальная политика регулирования сторонних взаимосвязей?	Нет
Существует ли в вашей компании программа уведомления о вопросах безопасности?	Да
Сколько процентов сотрудников участвовало в программе уведомления о вопросах безопасности?	Более 75 %
Какие темы охватывает обучение, связанное с осведомленностью?	Средства контроля и политики безопасности компании Оповещение о подозрительной активности Конфиденциальность Безопасность электронной почты, включая контроль спама и работу с вложениями
С какой периодичностью проводится обучение?	Ежегодно
Проводится ли тематическое обучение для служащих в зависимости от их роли в организации?	Нет

Глава 2. ОПИСАНИЕ СТРУКТУРЫ РАСПРЕДЕЛЕНИЯ АППАРАТНЫХ И ИНФОРМАЦИОННЫХ РЕСУРСОВ В ЛВС АИС ОБЪЕКТА ЗАЩИТЫ

При выполнении курсовой работы необходимо собрать и обобщить следующую информацию:

– описание подключения компьютеров к сетевому оборудованию и связи сетевого оборудования между собой (подключение с точностью до порта сетевого оборудования). Указывается в табличном виде по столбцам: номер ПК; описание подключения ПК к сетевому оборудованию; сетевое оборудование; описание подключения сетевого оборудования (табл. 2.1);

Таблица 2.1

Описание подключения компьютеров к сетевому оборудованию и связи сетевого оборудования между собой

Номер ПК	Описание подключения ПК к сетевому оборудованию	Сетевое оборудование	Описание подключения сетевого оборудования
Сеть головного офиса, коммутатор 1 (2-й этаж)			
1 2 3 4 8 9 10 11 13 14 15 33 34	Соединение рабочих мест с оборудованием выполнено четырехпарным одножильным медным кабелем «витая пара» категории 5е с использованием розетки RJ45. Применяемый протокол – Fast Ethernet на базе коммутатора	D-link DES-1008D Коммутатор с 24 портами 10/100Base-TX и двумя комбопортами 100/1000Base-T/SFP Скорость передачи данных Fast Ethernet – до 200 Мбит/с	Соединение выполнено четырехпарным одножильным медным кабелем «витая пара» категории 5е с использованием розетки RJ45. Применяемый протокол – Fast Ethernet на базе коммутатора
Сеть головного офиса, коммутатор 2 (3-й этаж)			
16 17 18 19 20	Соединение рабочих мест с оборудованием выполнено четырехпарным одножильным медным	D-link DES-1008D Коммутатор с 24 портами 10/100Base-TX и двумя комбопортами	Соединение выполнено четырехпарным одножильным медным кабелем «витая пара» категории 5е с использованием

Окончание табл. 2.1

Номер ПК	Описание подключения ПК к сетевому оборудованию	Сетевое оборудование	Описание подключения сетевого оборудования
21 23 24 25 26 27 28 29 30 31 32	кабелем «витая пара» категории 5е с использованием розетки RJ45. Применяемый протокол – Fast Ethernet на базе коммутатора	100/1000Base-T/SFP Скорость передачи данных Fast Ethernet – до 200 Мбит/с	розетки RJ 45. Применяемый протокол – Fast Ethernet на базе коммутатора
Сеть технологического отдела, коммутатор 3 (2-й этаж)			
5 6 7	Соединение рабочих мест с оборудованием выполнено четырехпарным одножильным медным кабелем «витая пара» категории 5е с использованием розетки RJ45. Применяемый протокол – Fast Ethernet на базе коммутатора	D-link DES-1008D Коммутатор с восемью портами 10/100 Мбит/с Скорость передачи данных Fast Ethernet – до 200 Мбит/с	Соединение выполнено четырехпарным одножильным медным кабелем «витая пара» категории 5е с использованием розетки RJ45. Применяемый протокол – Fast Ethernet на базе коммутатора

– описание адресного пространства локальной сети (ЛС): какие IP-адреса какими компьютерами используются при фиксированной адресации или какой диапазон IP-адресов выделен для организации ЛС (адреса ПК в каждом кабинете, администрации, бухгалтерии), для выхода в Интернет. Указывается в табличном виде по столбцам: номер кабинета; номер ПК; IP-адрес; принтер/МФУ; IP-адрес; сервер; IP-адрес (табл. 2.2);

Таблица 2.2

Описание адресного пространства ЛС

Номер кабинета	Номер ПК	IP-адрес	Принтер/ МФУ	IP-адрес	Сервер	IP-адрес
Сеть головного офиса, коммутатор 1 (2-й этаж)						
Касса	11	192.168.0.11	–	–	Сервер головного офиса	192.168.0.100
1	33	192.168.0.33	–	–		
	34	192.168.0.34	–	–		
2	1	192.168.0.1	KYOCERA ECOSYS M2735dn	192.168.0.422		
	2	192.168.0.2				
	3	192.168.0.3				
	4	192.168.0.4				
4	8	192.168.0.8	KYOCERA ECOSYS M2735dn	192.168.0.424		
	9	192.168.0.9				
	10	192.168.0.10				
6	14	192.168.0.14	–	–		
	13	192.168.0.13	–	–		
7	15	192.168.0.15	–	–		
Сеть головного офиса, коммутатор 2 (3-й этаж)						
1	16	192.168.0.16	–	–		
1а	17	192.168.0.17	–	–		
2	18	192.168.0.18	–	–		
	19	192.168.0.19	KYOCERA ECOSYS M2735dn	192.168.0.432		
	20	192.168.0.20				
	21	192.168.0.21				
4	23	192.168.0.23	KYOCERA ECOSYS M2735dn	192.168.0.434		
	24	192.168.0.24				
	25	192.168.0.25				
5	26	192.168.0.26	KYOCERA ECOSYS M2735dn	192.168.0.435		
	27	192.168.0.27				
	28	192.168.0.28				
	29	192.168.0.29				
6	30	192.168.0.30	KYOCERA ECOSYS M2735dn	192.168.0.436		
	31	192.168.0.31				
	32	192.168.0.32				
Сеть технологического отдела, коммутатор 3 (2-й этаж)						
3	5	192.168.1.5	KYOCERA ECOSYS M2735dn	192.168.1.423	Сервер технологического отдела	192.168.1.100
	6	192.168.1.6				
	7	192.168.1.7				

– описание учета аппаратных технических средств информатизации для серверов и рабочих станций. Указывается в табличном виде по столбцам: наименование; состав; инвентарный номер; расположение, номер кабинета; количество (табл. 2.3);

Таблица 2.3

Описание учета аппаратных технических средств информатизации для серверов и рабочих станций

Наименование	Состав	Инвентарный номер	Расположение, номер кабинета	Количество
АРМ	Моноблок – Lenovo IdeaCentre A340-24IGM Клавиатруа – Oklick 90M Black Мышь – Logitech M90		2-й этаж	32
		10011	Касса	
		10233	1	
		10234		
		10201	2	
		10202		
		10203		
		10204		
		10208	4	
		10209		
		10210		
		10214	6	
		10213		
		10215	7	
		10205	3	
		10206		
		10207		
		10309		
			3-й этаж	
		10316	1	
		10317	1а	
		10318	2	
		10321		
		10323	4	
		10324		
		10325		
		10326	5	
		10330	6	
		10331		
		10332		
Сервер головного офиса	HPE ProLiant DL360 Gen10	10100	5, 2-й этаж	1
Сервер технологического отдела	HPE ProLiant DL360 Gen10	10101	5, 2-й этаж	1

– описание учета аппаратных технических средств активного сетевого оборудования (концентраторов, коммутаторов и маршрутизаторов). Указывается в табличном виде по столбцам: наименование; состав; инвентарный номер; расположение, номер кабинета; количество (табл. 2.4);

Таблица 2.4

Описание учета аппаратных технических средств активного сетевого оборудования

Наименование	Состав	Инвентарный номер	Расположение, номер кабинета	Количество
Коммутатор	D-link DES-1008D, 8 портов	10102	3, 2-й этаж	1
	D-link DES-1026G, 24 порта	10103	5, 2-й этаж	2
		10104	5, 3-й этаж	

– описание учета аппаратных периферийных технических средств (принтеры, сканеры, плоттеры, графопостроители и пр.). Указывается в табличном виде по столбцам: наименование; состав; инвентарный номер; расположение, номер кабинета; количество (табл. 2.5);

Таблица 2.5

Описание учета аппаратных периферийных технических средств

Наименование	Состав	Инвентарный номер	Расположение, номер кабинета	Количество
МФУ	KYOCERA ECOSYS M2735dn		2-й этаж	14
		10105	2	
		10106	3	
		10107	4	
		10115	6	
		10116		
		10117	7	
		10118	1	
			3-й этаж	
		10108	2	
		10114		
		10109	4	
		10101	5	
		10111	6	
		10112	1	
		10113	1а	
Принтер	Xerox B210	10118	Касса	1

– описание учета программного обеспечения, установленного на компьютерах ЛВС. Указывается в табличном виде по столбцам: наименование ПО; номер лицензии; компьютеры отдела; расположение (табл. 2.6);

Таблица 2.6

Описание учета программного обеспечения, установленного на компьютерах ЛВС

Наименование ПО	Номер лицензии	Компьютеры отдела	Расположение
LibreOffice	Бесплатная	Все АРМ	Все кабинеты
1С: Склад	Серверная XXXXXXXX	Бухгалтерия ПК 1, 2, 3, 4 Маркетинговый отдел ПК 19, 20, 21 Финансовый отдел ПК 8, 9, 10	2-й, 3-й этаж
1С: Бухгалтерия	Серверная XXXXXXXX	Бухгалтерия ПК 1, 2, 3, 4 Маркетинговый отдел ПК 19, 20, 21 Финансовый отдел ПК 8, 9, 10 Кадры ПК 30, 31, 32	2-й, 3-й этаж
1С: Кадры	Серверная XXXXXXXX	Бухгалтерия ПК 1, 2, 3, 4 Кадры ПК 30, 31, 32	2-й, 3-й этаж
1С: Зарплата	Серверная XXXXXXXX	Бухгалтерия ПК 1, 2, 3, 4 Финансовый отдел ПК 8, 9, 10 Кадры ПК 30, 31, 32	2-й, 3-й этаж
ПО для специального производственного оборудования, работающего с силиконом	XXXXXXXXX	Технологический отдел ПК 7	3-й, 2-й этаж
Autodesk 3ds Max	XXXXXXXXX, XXXXXXXXX, XXXXXXXXX	Технологический отдел ПК 5,6	3-й, 2-й этаж
Kaspersky Endpoint Security 11	Серверная на 40 рабочих мест XXXXXXXXXXX	Все АРМ головного офиса	Все кабинеты головного офиса

– подтверждение лицензионной чистоты программного обеспечения. Указывается в табличном виде по столбцам: номер кабинета; номер ПК; тип ПО; необходимость лицензии и срок; периодичность обновления (табл. 2.7);

Таблица 2.7

Подтверждение лицензионной чистоты программного обеспечения на компьютерах ЛВС

Номер кабинета	Номер ПК	Тип ПО	Необходимость лицензии и срок	Периодичность обновления
Касса	11	Системное ПО (ОС)… Офис… Прикладное ПО Продукты 1С Антивирус Касперского	Лицензия XXXXXXXXXXX Бесплатное ПО Лицензия XXXXXXXXXXX Лицензия XXXXXXXXXXX	Не требуется Ключи защиты менять один раз в неделю для ПК, не имеющих выхода в Интернет
1	33			
1	34			
2	1			
2	2			
2	3			
2	4			
4	8			
4	9			
4	10			
6	14			
6	13			
7	15			
1	16			
1а	17			
2	18			
2	19			
2	20			
2	21			
4	23			
4	24			
4	25			
5	26			
5	27			
5	28			
5	29			
6	30			
6	31			
6	32			

– документы по организации доступа к глобальным сетям и сети Интернет. Указывается в табличном виде по столбцам: номер ПК; IP-адрес; выход в Интернет; выход во внутреннюю сеть (табл. 2.8).

Таблица 2.8

Выход компьютеров в локальные и глобальные сети

Номер ПК	IP-адрес	Выход в Интернет	Выход во внутреннюю сеть
11	192.168.0.11	Имеется	Имеется
33	192.168.0.33		
34	192.168.0.34		
1	192.168.0.1		
2	192.168.0.2		
3	192.168.0.3		
4	192.168.0.4		
8	192.168.0.8		
9	192.168.0.9		
10	192.168.0.10		
14	192.168.0.14		
13	192.168.0.13		
15	192.168.0.15		
16	192.168.0.16		
17	192.168.0.17		
18	192.168.0.18		
19	192.168.0.19		
20	192.168.0.20		
21	192.168.0.21		
23	192.168.0.23		
24	192.168.0.24		
25	192.168.0.25		
26	192.168.0.26		
27	192.168.0.27		
28	192.168.0.28		
29	192.168.0.29		
30	192.168.0.30		
31	192.168.0.31		
32	192.168.0.32		
5	192.168.1.5	Не имеется	Имеется
6	192.168.1.6		
7	192.168.1.7		

Глава 3. ФОРМИРОВАНИЕ МАТРИЦЫ И МОДЕЛИ ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ АИС

В ходе выполнения курсовой работы студент должен собрать и обобщить следующую информацию:

– для таблицы исходных данных структуры защищаемой информации на каждом компьютере ЛВС (какие информационные ресурсы где находятся и какой степени конфиденциальности) и таблицы используемого ПО на ПК необходимо определить, какие информационные ресурсы будут свободно использоваться всеми сотрудниками организации и всеми посетителями, а какие ресурсы будут ограниченного доступа и только для определенных сотрудников организации. Информацию представить в табличном виде;

– для таблицы исходных данных структуры защищаемой информации на каждом компьютере ЛВС (какие информационные ресурсы где находятся и какой степени конфиденциальности) необходимо определить применяемую систему организации распределения доступа (дискреционное, мандатное или ролевое разграничение доступа). Для выбранных систем определить необходимые программно-аппаратные средства организации доступа. Информацию представить в табличном виде;

– для каждого компьютера (его информационных ресурсов ограниченного доступа) и каждого пользователя этого компьютера – сотрудника организации выбрать модели доступа к информационным ресурсам, способы и технические средства организации распределения доступа (при необходимости) и способы прохождения идентификации и аутентификации. Информацию представить в табличном виде;

– для организации удаленного доступа к информационным ресурсам организации через глобальную сеть Интернет определить необходимые программные средства организации доступа. Информацию представить в табличном виде.

Типы и объекты информатизации, на которых размещены ресурсы ограниченного доступа, приведены в исходных данных структуры защищаемой информации (табл. 1.2). На каждом компьютере ЛВС ООО «Пример» применяется система организации распределения доступа, основанная на встроенных в ОС Windows механизмах разграничения доступа (доменная политика). Модель доступа к информационным ресурсам представлена в таблице.

Модель доступа к информационным ресурсам

Структурное подразделение	Имя пользователя	Имеет доступ на ПК (номер ПК)	БД «Склад»	БД «Бухгалтерия»	БД «Кадры»	БД «Зарплата»	БД «Рецептура и инструкция изготовления изделия из силикона»	БД «Собственные наработки 3D-моделей»	Интернет
Руководство	Gen-dir	16	r	r	+	+	-	-	+
Руководство	zam_econ	18	r	+	r	r	-	-	+
Канцелярия	Zav_kanc	14, 17, 15	-	-	-	-	-	-	+
Канцелярия	secretar	17, 14, 15	-	-	-	-	-	-	+
Канцелярия	archiv	15, 14	-	-	-	-	-	-	+
Служба безопасности	Nach_otd _bezopas	23, 24, 13, 25, 26, 27	-	-	r	-	-	-	+
Служба безопасности	Bezopas_1	24	-	-	r	-	-	-	+
Служба безопасности	Inspector _KI	13, 14, 17, 15	-	-	r	-	-	-	+
Служба безопасности	Bezopas_2	Все (1 – 34)	-	-	-	-	-	-	+
Служба безопасности	Bezopas_3	26, 27	-	-	-	-	-	-	+
Служба безопасности	Bezopas_4	27, 26	-	-	-	-	-	-	+
Служба безопасности	Bezopas_5	28, 29	-	-	-	-	-	-	+
Служба безопасности	Bezopas_6	29, 28	-	-	-	-	-	-	+
Технологический отдел	teh_otd_1	5, 6, 7	-	-	-	-	+	+	-
Технологический отдел	teh_otd_2	6, 7	-	-	-	-	r	+	-
Технологический отдел	teh_otd_3	7, 6	-	-	-	-	r	+	-
Служба автоматизации (IT)	IT-1	Все (1 – 34)	-	-	-	-	-	-	+
Служба автоматизации (IT)	IT-2	Все (1 – 34)	-	-	-	-	-	-	+
Отдел кадров и организационно-правовой работы	Nach_ otd_kadri	30, 31, 32	-	+	+	+	-	-	+

Окончание

Структурное подразделение	Имя пользователя	Имеет доступ на ПК (номер ПК)	БД «Склад»	БД «Бухгалтерия»	БД «Кадры»	БД «Зарплата»	БД «Рецептура и инструкция изготовления изделия из силикона»	БД «Собственные наработки 3D-моделей»	Интернет
Отдел кадров и организационно-правовой работы	Kadri_1	31, 32	-	+	+	+	-	-	+
Отдел кадров и организационно-правовой работы	Kadri_2	32, 31	-	+	+	+	-	-	+
Бухгалтерия	Glav_buh	8, 9, 10, 11	-	+	r	+	-	-	+
Бухгалтерия	Buh_1	9, 10, 11	-	+	r	+	-	-	+
Бухгалтерия	Buh_2	10, 11	-	+	r	+	-	-	+
Бухгалтерия	Kassir	11, 10	-	+	r	+	-	-	+
Отдел маркетинга	Market-1	19, 20, 21	+	r	-	-	-	-	+
Отдел маркетинга	Market-2	20, 21	+	r	-	-	-	-	+
Отдел маркетинга	Market-3	21, 20	+	r	-	-	-	-	+
Финансово-экономический отдел	Fin_otd-1	1, 2, 3, 4	-	+	+	+	-	-	+
Финансово-экономический отдел	Fin_otd-2	2, 3, 4	-	+	+	+	-	-	+
Финансово-экономический отдел	Fin_otd-3	3, 4	-	+	+	+	-	-	+
Финансово-экономический отдел	Fin_otd-4	4, 3	-	+	+	+	-	-	+

Примечание. Система организации распределения доступа – ролевое разграничение доступа: - – нет доступа; + – полный доступ; r – чтение; w – запись.

Глава 4. КЛАССИФИКАЦИЯ АИС ПРЕДПРИЯТИЯ ПО ТРЕБОВАНИЯМ РУКОВОДЯЩЕГО ДОКУМЕНТА ФСТЭК РОССИИ

Классификация АИС предприятия основана на требованиях руководящего документа ФСТЭК России от 30 марта 1992 г. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». В нем приведены два определения понятия АИС.

Автоматизированная информационная система – совокупность информации, экономико-математических методов и моделей, технических, программных, технологических средств и специалистов, предназначенная для обработки информации и принятия управленческих решений.

Автоматизированная информационная система – взаимосвязанная совокупность данных, оборудования, программных средств, персонала, стандартов, процедур, предназначенных для сбора, обработки, распределения, хранения, выдачи (предоставления) информации в соответствии с требованиями, вытекающими из целей организации.

К числу определяющих признаков, по которым АС группируются в различные классы, относятся:

– наличие в АС информации различного уровня конфиденциальности;

– уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;

– режим обработки данных в АС (коллективный или индивидуальный).

Устанавливается девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Третья группа включает в себя АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на

носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А.

Вторая группа включает в себя АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса – 2Б и 2А.

Первая группа включает в себя многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А.

Необходимые исходные данные для проведения классификации конкретной АС следующие:

– перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;

– перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;

– матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;

– режим обработки данных в АС.

Класс АС выбирается заказчиком и разработчиком с привлечением специалистов по защите информации.

Пример классификации АИС предприятия по требованиям руководящего документа ФСТЭК России представлен в таблице.

Классификация АИС предприятия по требованиям руководящего документа ФСТЭК от 30 марта 1992 г.

Номер ПК и сервера	Номер помещения	Пользователи АИС	Установленное ПО	Наименование АИС	Класс защищенности АИС
Сервер технологического отдела, ПК 5, 6, 7	3, 2-й этаж	teh_otd_1, teh_otd_2, teh_otd_3	ПО для специального производственного оборудования, Autodesk 3ds Max	Производство	1Г

Окончание

Номер ПК и сервера	Номер помещения	Пользователи АИС	Установленное ПО	Наименование АИС	Класс защищенности АИС
Сервер головного офиса, ПК 1, 2, 3, 4, 8, 9, 10, 11, 18, 16	2, 4, касса, 2-й этаж; 1, 2, 3-й этаж	Gen-dir, zam_econ, Fin_otd-1, Fin_otd-2, Fin_otd-3, Fin_otd-4, Glav_buh, Buh_1, Buh_2, kassir	1С: Бухгалтерия, 1С: Кадры, 1С: Зарплата, LibreOffice, Kaspersky Endpoint Security 11	Бухгалтерия	1Б
Сервер головного офиса, ПК 1, 2, 3, 4, 8, 9, 10, 18, 16	2, 4, 2-й этаж; 1, 2, 3-й этаж	Gen-dir, zam_econ, Fin_otd-1, Fin_otd-2, Fin_otd-3, Fin_otd-4, Glav_buh, Buh_1, Buh_2	1С: Бухгалтерия, 1С: Кадры, 1С: Склад, LibreOffice, Kaspersky Endpoint Security 11	Финансы и планирование	1Б
Сервер головного офиса, ПК 30, 31, 32	1, 6, 3-й этаж	Gen-dir, Nach_otd_kadri, Kadri_1, Kadri_2	1С: Бухгалтерия, 1С: Кадры, LibreOffice, Kaspersky Endpoint Security 11	Кадры	1Б
Сервер головного офиса, ПК 16, 18, 1, 2, 3, 4, 19, 20, 21	1, 2, 3-й этаж 2, 2-й этаж	Gen-dir, zam_econ, Fin_otd-1, Fin_otd-2, Fin_otd-3, Fin_otd-4, Market-1, Market-2, Market-3	1С: Бухгалтерия, 1С: Склад, LibreOffice, Kaspersky Endpoint Security 11	Маркетинг	1Б
Сервер головного офиса, ПК 31, 32	1, 2-й этаж	IT-1, IT-2	LibreOffice, Kaspersky Endpoint Security 11	Администрирование	1Б
Сервер головного офиса, ПК 23, 24, 13, 25, 26, 27, 28, 29	4, 5, 3-й этаж; 6, 2-й этаж	Nach_otd_bezopas, Bezopas_1, Bezopas_2, Bezopas_3, Bezopas_4, Bezopas_5, Bezopas_6, Inspector_	LibreOffice, Kaspersky Endpoint Security 11	Безопасность	1А

Глава 5. ФОРМИРОВАНИЕ МОДЕЛИ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АИС НА ПРЕДПРИЯТИИ

Уровни возможностей нарушителей по реализации угроз безопасности информации приведены в приложении 8 «Методики оценки угроз безопасности информации» ФСТЭК России (2021 г.) [11]. Данный документ имеется на сайте ФСТЭК России и выдается студентам в электронном виде. Всего выделяют четыре типа нарушителей: Н1 – нарушитель, обладающий базовыми возможностями; Н2 – нарушитель, обладающий базовыми повышенными возможностями; Н3 – нарушитель, обладающий средними возможностями; Н4 – нарушитель, обладающий высокими возможностями. *Нарушителями могут быть (виды):*

– физическое лицо (хакер);

– лица, отвечающие за поставку программных, программно-аппаратных средств, обеспечивающих систем;

– лица, отвечающие за функционирование систем и сетей или обеспечивающих систем (администрация, охрана, уборщики и т. д.);

– авторизованные пользователи систем и сетей;

– бывшие работники (пользователи);

– преступные группы (два лица и более, действующие по единому плану);

– конкурирующие организации;

– поставщики вычислительных услуг, услуг связи;

– лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;

– системные администраторы и администраторы безопасности;

– террористические, экстремистские группировки;

– разработчики программных, программно-аппаратных средств;

– специальные службы иностранных государств.

Примеры определения актуальных нарушителей при реализации угроз безопасности информации и соответствующих им возможностей приведены в приложении 9 «Методики оценки угроз безопасности информации» ФСТЭК России (2021 г.) [Там же]. В указанном приложении в табличном виде приведены виды риска (ущерба) и возможные

негативные последствия, виды актуального нарушителя, категории нарушителя (внутренний или внешний), уровни возможностей нарушителя (Н1 – Н4).

Примеры определения актуальных способов реализации угроз безопасности информации, соответствующих им видов нарушителей и их возможностей приведены в приложении 10 «Методики оценки угроз безопасности информации» ФСТЭК России (2021 г.) [11].

В указанном приложении в табличном виде приведены вид нарушителя, категории нарушителя, объекты воздействия, доступные интерфейсы, способы реализации.

Порядок формирования модели нарушителя информационной безопасности в АИС на предприятии следующий.

1. На основе анализа всех исходных данных по объекту защиты определить виды актуальных нарушителей для заданного объекта защиты и их типы, какие информационные ресурсы будут подвергаться воздействию со стороны каких нарушителей.

2. Составить таблицу определения актуальных нарушителей при реализации угроз безопасности информации и соответствующих им возможностей для объекта защиты. Форму таблицы принять в соответствии с приложением 9 «Методики оценки угроз безопасности информации» ФСТЭК России (2021 г.) (табл. 5.1).

3. Составить таблицу определения актуальных способов реализации угроз безопасности информации, соответствующих им видов нарушителей и их возможностей для объекта защиты. Форму таблицы принять в соответствии с приложением 10 «Методики оценки угроз безопасности информации» ФСТЭК России (2021 г.) (табл. 5.2).

Содержание отчета: пояснительная записка с обоснованием выбора актуальных нарушителей для заданного объекта защиты и определением их типов, обоснованием видов информационных ресурсов объекта защиты, которые могут подвергаться воздействию со стороны нарушителей. При этом необходимо обосновать, со стороны каких типов и видов нарушителей возможно посягательство.

Таблица 5.1

Определение актуальных нарушителей при реализации угроз безопасности информации и соответствующих им возможностей для объекта защиты

№ п/п	Виды риска (ущерба) и возможные негативные последствия	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
1	Нарушение конфиденциальности (утечка) персональных данных (У1)	Преступные группы (криминальные структуры)	Внешний Внутренний	Н3
		Отдельные физические лица	Внешний	Н2
		Разработчики программных, программно-аппаратных средств	Внутренний	Н3
		Системные администраторы и администраторы безопасности	Внутренний	Н2
		Авторизованные пользователи систем и сетей	Внутренний	Н2
		Системные администраторы и администраторы безопасности	Внутренний	Н2
		Бывшие работники (пользователи)	Внешний	Н1
2	Разглашение персональных данных граждан (У1)	Преступные группы (криминальные структуры)	Внешний Внутренний	Н3
		Отдельные физические лица	Внешний	Н2
		Разработчики программных, программно-аппаратных средств	Внутренний	Н3
		Авторизованные пользователи систем и сетей	Внутренний	Н2
		Системные администраторы и администраторы безопасности	Внутренний	Н2
		Бывшие работники (пользователи)	Внешний	Н1
3	Потеря (хищение) денежных средств (У2)	Преступные группы (криминальные структуры)	Внешний Внутренний	Н3
		Отдельные физические лица (хакеры)	Внешний	Н2
		Авторизованные пользователи систем и сетей	Внутренний	Н2
		Системные администраторы и администраторы безопасности	Внутренний	Н2

Продолжение табл. 5.1

№ п/п	Виды риска (ущерба) и возможные негативные последствия	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
4	Недополучение ожидаемой (прогнозируемой) прибыли Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса (У2)	Отдельные физические лица (хакеры)	Внешний	Н2
		Конкурирующие организации	Внешний	Н2
		Разработчики программных, программно-аппаратных средств	Внутренний	Н3
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2
		Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т. д.)	Внутренний	Н1
5	Срыв запланированной сделки с партнером (У2)	Конкурирующие организации	Внешний	Н2
		Авторизованные пользователи систем и сетей	Внутренний	Н2
		Системные администраторы и администраторы безопасности	Внутренний	Н2
6	Причинение имущественного ущерба (У2)	Террористические, экстремистские группировки	Внешний	Н3
		Преступные группы (криминальные структуры)	Внешний	Н3
7	Потеря конкурентного преимущества (У2)	Отдельные физические лица (хакеры)	Внешний	Н2
		Конкурирующие организации	Внешний	Н2
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2
		Авторизованные пользователи систем и сетей	Внутренний	Н2
		Бывшие работники (пользователи)	Внешний	Н1
8	Неспособность выполнения договорных обязательств (У2)	Террористические, экстремистские группировки	Внешний	Н3
		Преступные группы (криминальные структуры)	Внешний	Н3

Окончание табл. 5.1

№ п/п	Виды риска (ущерба) и возможные негативные последствия	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
8	Неспособность выполнения договорных обязательств (У2)	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2
		Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т. д.)	Внутренний	Н1
		Авторизованные пользователи систем и сетей	Внутренний	Н2
9	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций) (У2)	Террористические, экстремистские группировки	Внешний	Н3
		Преступные группы (криминальные структуры)	Внешний	Н3
		Отдельные физические лица (хакеры)	Внешний	Н2
		Поставщики вычислительных услуг, услуг связи	Внутренний	Н2
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2
		Авторизованные пользователи систем и сетей	Внутренний	Н2
10	Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.) (У2)	Террористические, экстремистские группировки	Внешний	Н3
		Преступные группы (криминальные структуры)	Внешний Внутренний	Н3
		Разработчики программных, программно-аппаратных средств	Внутренний	Н3
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2
		Отдельные физические лица (хакеры)	Внешний	Н2
		Авторизованные пользователи систем и сетей	Внутренний	Н2
		Системные администраторы и администраторы безопасности	Внутренний	Н2
		Бывшие работники (пользователи)	Внешний	Н1

Таблица 5.2

Определение актуальных способов реализации угроз безопасности информации и соответствующих им видов нарушителей, их возможностей для объекта защиты

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
1	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т. д.) (Н1)	Внутренний	Оборудование технологического отдела	Доступ в помещение с оборудованием. Физический контакт с оборудованием технологического отдела	Нанесение вреда или ущерба производственному оборудованию умышленно или по неосторожности
2	Бывшие работники (пользователи) (Н1)	Внешний	Конфиденциальные данные завода. Персональные данные работников. Коммерческая тайна завода, включая рецептуру изготовления силиконовых изделий	Информация стала доступна во время исполнения работником служебных обязанностей	Продажа ценной информации заинтересованным лицам, конкурентам Разглашение информации различными способами распространения информации
3	Отдельные физические лица (хакеры) (Н2)	Внешний	Удаленное автоматизированное рабочее место (АРМ) пользователя: несанкционированный доступ к операционной системе АРМ пользователя; нарушение конфиденциальности информации, содержащейся на АРМ пользователя	Доступ через локальную вычислительную сеть организации	Внедрение вредоносного программного обеспечения
				Съемные машинные носители информации, подключаемые к АРМ пользователя	Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя

Продолжение табл. 5.2

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
3	Отдельные физические лица (хакеры) (Н2)	Внешний	Веб-сайт, интернет-магазин завода: отказ в обслуживании веб-сайта	Веб-интерфейс пользователя веб-сайта государственных услуг	Использование уязвимостей кода программного обеспечения веб-сервера
					Внедрение вредоносного кода в веб-приложение
				Сетевые интерфейсы коммутатора сети, где расположен веб-сервер	Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя
4	Системные администраторы и администраторы безопасности (Н2)	Внутренний	АСУ химического завода, информационная система (ИС), БД	Интерфейс АСУ	Несанкционированное отключение средств защиты Установка ПО, не связанного с исполнением служебных обязанностей
5	Авторизованные пользователи систем и сетей (Н2)	Внутренний	АРМ пользователя, сейф с хранящейся информацией (в пределах доступа пользователя)	Веб-интерфейс пользователя, физический доступ в помещения с конфиденциальной информацией	Кража носителей информации Кражи, модификации, уничтожение информации Непреднамеренная модификация (уничтожение) информации сотрудниками

Продолжение табл. 5.2

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
6	Конкурирующие организации (Н2)	Внешний Внутренний	Информация, содержащая коммерческую тайну	Интерфейсы, доступные пользователю сети головного офиса Физический доступ в помещения с конфиденциальной информацией	Кража носителей информации Анализ сетевого трафика с перехватом передаваемой из информационной системы персональных данных (ИСПДн) и принимаемой из внешних сетей информации с нарушителем внутри контролируемой зоны
7	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ (Н2)	Внутренний	Нарушение конфиденциальности информации, содержащейся на АРМ пользователя	Локальная сеть, АРМ пользователей головного офиса и технологического отдела	Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ
8	Поставщики вычислительных услуг, услуг связи (Н2)	Внутренний	Нарушение конфиденциальности информации, содержащейся на АРМ пользователя Модификация информации	–	Недекларированные возможности системного ПО и ПО для обработки персональных данных
9	Преступные группы (криминальные структуры) (Н3)	Внешние Внутренний	–	–	Анализ сетевого трафика с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации с нарушителем внутри контролируемой зоны

Окончание табл. 5.2

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
9			–	–	Навязывание ложного маршрута сети
10	Террористические, экстремистские группировки (Н3)	Внешний	Вычислительные мощности серверов, сети	–	Навязывание ложного маршрута сети Подмены доверенного объекта в сети
11	Разработчики программных, программно-аппаратных средств (Н3)	Внутренний	Нарушение конфиденциальности информации Вычислительные мощности серверов, сети	–	Кражи, модификации, уничтожение информации Навязывание ложного маршрута сети Подмены доверенного объекта в сети

Глава 6. ОПРЕДЕЛЕНИЕ КЛАССА ЗАЩИЩЕННОСТИ АИС И СОСТАВА БАЗОВЫХ МЕР ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ СООТВЕТСТВУЮЩЕГО КЛАССА ЗАЩИЩЕННОСТИ

6.1. Общие положения

Класс защищенности информационной системы и состав базовых мер защиты информации (не содержащей сведений, составляющих государственную тайну) для соответствующего класса защищенности определяют согласно приказам ФСТЭК России № 17 (2013 г.) и № 27 (2017 г.). Приказом ФСТЭК России № 17 (2013 г.) устанавливаются требования к обеспечению защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней (далее – защита информации) при обработке указанной информации в государственных информационных системах. Этим документом устанавливаются также классы защищенности информационной системы (приложение 1 приказа ФСТЭК № 17 (2013 г.)).

Класс защищенности информационной системы (первый класс (К1), второй класс (К2), третий класс (К3)) определяется в зависимости от уровня значимости (УЗ) информации, обрабатываемой в этой информационной системе, и масштаба информационной системы (федеральный, региональный, объектовый).

Класс защищенности (К) = [уровень значимости информации; масштаб системы].

Уровень значимости информации обусловлен степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации.

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)],

где степень возможного ущерба определяется обладателем информации (заказчиком) и (или) оператором самостоятельно экспертным или иными методами и может быть:

– высокой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции;

– средней, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций;

– низкой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

Информация имеет высокий уровень значимости (УЗ 1), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба. Информация имеет средний уровень значимости (УЗ 2), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба. Информация имеет низкий уровень значимости (УЗ 3), если для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определены низкие степени ущерба.

Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы определяются в соответствии с приложением 2 приказа ФСТЭК России № 17 (2013 г.).

Приказом ФСТЭК России № 27 (2017 г.) вносятся изменения в приказ ФСТЭК России № 17 (2013 г.). Данные документы имеются на сайте ФСТЭК России и выдаются студентам в электронном виде, причем приказ ФСТЭК России № 17 (2013 г.) приведен уже в редакции приказа ФСТЭК России № 27 (2017 г.).

Порядок определения класса защищенности информационной системы и состава базовых мер защиты следующий.

1. После выбора информационных систем объекта защиты провести оценку уровня значимости информации в каждой ИС по методике приложения 1 приказа ФСТЭК России № 17 (2013 г.) в редакции приказа ФСТЭК России № 27 (2017 г.).

2. После выбора масштаба ИС (федеральный, региональный, объектовый) и уровня значимости информации в ИС провести оценку класса защищенности для каждой информационной системы объекта защиты в соответствии с приложением 1 приказа ФСТЭК России № 17 (2013 г.) в редакции приказа ФСТЭК России № 27 (2017 г.).

3. Для информационной системы провести анализ состава мер защиты информации и их базовых наборов для соответствующего класса защищенности информационной системы по методике приложения 2 приказа ФСТЭК России № 17 (2013 г.) в редакции приказа ФСТЭК России № 27 (2017 г.). Обобщенные сведения представить в табличном виде по форме таблицы приложения 2 для информационной системы объекта защиты.

Содержание отчета: пояснительная записка с обоснованием оценки класса защищенности для каждой информационной системы объекта защиты в соответствии с приложением 1 приказа ФСТЭК России № 17 (2013 г.) в редакции приказа ФСТЭК России № 27 (2017 г.).

6.2. Пример определения класса защищенности АИС и состава базовых мер защиты информации для соответствующего класса защищенности

Пояснительная записка с обоснованием оценки класса защищенности для каждой информационной системы ООО «Пример» приведена ниже.

Для определения класса защищенности информационных систем ООО «Пример» был использован приказ ФСТЭК России № 17 (2013 г.) в редакции приказа ФСТЭК России № 27 (2017 г.).

Уровень значимости информации определяется степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации.

Если при обработке информационных ресурсов в информационной системе имеется два и более вида информации, уровень значимости информации определятся отдельно для каждого вида информации (табл. 6.1).

Таблица 6.1

Наименование ИС	Вид обрабатываемой информации	Уровень значимости (УЗ)
Производство	КТ	Низкий (УЗ 3)
Бухгалтерия	ПДн, служебная тайна, налоговая тайна	Низкий (УЗ 3)
Финансы и планирование	ПДн, служебная тайна, КТ	Низкий (УЗ 3)
Кадры	ПДн, налоговая тайна	Низкий (УЗ 3)
Маркетинг	КТ	Низкий (УЗ 3)
Администрирование	Служебная тайна	Низкий (УЗ 3)
Безопасность	Служебная тайна	Низкий (УЗ 3)

Степень возможного ущерба определена как низкая, так как в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в социальной, экономической, финансовой областях деятельности и информационные системы могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств. Информация имеет низкий уровень значимости (УЗ 3), если для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определена низкая степень ущерба. Итоговый уровень значимости информации, обрабатываемой в информационной системе, устанавливается по наивысшим значениям степени возможного ущерба, определенным для конфиденциальности, целостности, доступности каждого вида информации.

Все перечисленные информационные системы ООО «Пример» имеют объектовый масштаб, так как они функционируют на объектах одной организации и не имеют сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях.

В соответствии с таблицей приложения 1 приказа ФСТЭК России № 17 (2013 г.) (в ред. приказа ФСТЭК России от 15.02.2017 г. № 27) были определены следующие классы защищенности информационных систем:

производство – К3
бухгалтерия – К3
финансы и планирование – К3
кадры – К3
маркетинг – К3
администрирование – К3
безопасность – К3

Если рассматривать класс защищенности для информационной системы ООО «Пример» в целом с учетом отдельных сегментов и составляющих ИС, то имеем класс защищенности К3.

Таблица 6.2

Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы

Условное обозначение и номер меры	Мера защиты информации в информационных системах	Класс защищенности информационной системы	Наличие меры защиты
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)			
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	3	Да
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	3	Да
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	3	Да

Продолжение табл. 6.2

Условное обозначение и номер меры	Мера защиты информации в информационных системах	Класс защищенности информационной системы	Наличие меры защиты
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	3	Да
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	3	Нет
II. Управление доступом субъектов доступа к объектам доступа (УПД)			
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	3	Да
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	3	Да
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	3	Да
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	3	Да
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	3	Да
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	3	Нет
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	3	Да
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	3	Да

Продолжение табл. 6.2

Условное обозначение и номер меры	Мера защиты информации в информационных системах	Класс защищенности информационной системы	Наличие меры защиты
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	3	Нет
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	3	Нет
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	3	Нет
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	3	Нет
III. Ограничение программной среды (ОПС)			
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	3	Да
IV. Защита машинных носителей информации (ЗНИ)			
ЗНИ.1	Учет машинных носителей информации	3	Да
ЗНИ.2	Управление доступом к машинным носителям информации	3	Да
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)	3	Да
V. Регистрация событий безопасности (РСБ)			
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	3	Да
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	3	Да
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	3	Да

Продолжение табл. 6.2

Условное обозначение и номер меры	Мера защиты информации в информационных системах	Класс защищенности информационной системы	Наличие меры защиты
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе на аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнение объема (емкости) памяти	3	Да
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	3	Да
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	3	Да
РСБ.7	Защита информации о событиях безопасности	3	Да
VI. Антивирусная защита (АВЗ)			
АВЗ.1	Реализация антивирусной защиты	3	Да
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	3	Да
VIII. Контроль (анализ) защищенности информации (АНЗ)			
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	3	Да
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	3	Да
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	3	Да
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	3	Да
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе	3	Да

Продолжение табл. 6.2

Условное обозначение и номер меры	Мера защиты информации в информационных системах	Класс защищенности информационной системы	Наличие меры защиты
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)			
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	3	Да
XI. Защита среды виртуализации (ЗСВ)			
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	3	Да
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	3	Да
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	3	Да
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	3	Да
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей	3	Да
XII. Защита технических средств (ЗТС)			
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования	3	Да

Окончание табл. 6.2

Условное обозначение и номер меры	Мера защиты информации в информационных системах	Класс защищенности информационной системы	Наличие меры защиты
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации, средствам обеспечения функционирования информационной системы и в помещения и сооружения, в которых они установлены	3	Да
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	3	Да
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)			
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе по беспроводным каналам связи	3	Да
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	3	Да
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	3	Да
ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе	3	Нет

Глава 7. ПРОВЕДЕНИЕ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АИС С ИСПОЛЬЗОВАНИЕМ СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ MICROSOFT SECURITY ASSESSMENT TOOL

7.1. Общие положения

MSAT – это обновленная версия средства Microsoft Security Risk Self-Assessment Tool (MSRSAT), выпущенного в 2004 г., и средства Microsoft Security Assessment Tool 2.0, выпущенного в 2006 г. Это ПО служит для создания комплексного инструментария, способного предоставлять достоверную информацию о проблемах безопасности, которые могут возникнуть в организации.

Данное средство использует целостный подход к оценке системы безопасности, анализируя влияние человеческого фактора, процессов и технологий. Полученные результаты предоставляются пользователям вместе с подробным руководством, рекомендациями по снижению угроз и ссылками на отраслевые руководства, содержащие дополнительные сведения, которые могут помочь организациям получить информацию о средствах и методах, способных повысить безопасность ИТ-среды организации. Microsoft Security Assessment Tool позволяет оценить следующие характеристики:

– профиль риска для бизнеса;

– многоуровневую защиту.

Вопросы, содержащиеся во входящей в состав средства анкете, и сопоставленные им ответы получены на основании анализа общепринятых передовых методик обеспечения безопасности, используемых для решения как типичных, так и специализированных задач. Предлагаемые MSAT вопросы и рекомендации основаны на существующих стандартах (ISO 17799 и NIST), на рекомендациях и руководстве группы Trustworthy Computing Group корпорации Майкрософт и других используемых в отрасли рекомендациях по обеспечению безопасности.

Ответив на вопросы, пользователь может просмотреть подробный отчет, сформированный на основании результатов опроса, и сравнить полученные результаты с результатами других опросов, проводившихся в выбранной отрасли или компаниях выбранного размера.

MSAT поддерживают операционные системы Windows 7, Windows Server 2003 Service Pack 2, Windows Server 2008 и выше.

Для работы MSAT подключение к Интернету не требуется, однако для передачи результатов опроса и проверки наличия обновлений необходим доступ в Интернет.

Содержание отчета: в процессе проведения аудита АИС необходимо последовательно ответить на вопросы в ПО MSAT о защищаемой АИС с использованием исходных данных, информации, собранной по разделам отчета 1 – 6. По окончании проведения аудита формируется отчет о состоянии информационной безопасности АИС с рекомендациями по ее повышению.

7.2. Пример аудита информационной безопасности АИС с использованием специализированного программного обеспечения Microsoft Security Assessment Tool

Аудит приведен на основе собранной информации об ООО «Пример» в разделах отчета 1 – 6.

Сводный отчет. Профиль риска для бизнеса (ПРБ) и индекс эшелонированной защиты представлены на рис. 7.1.

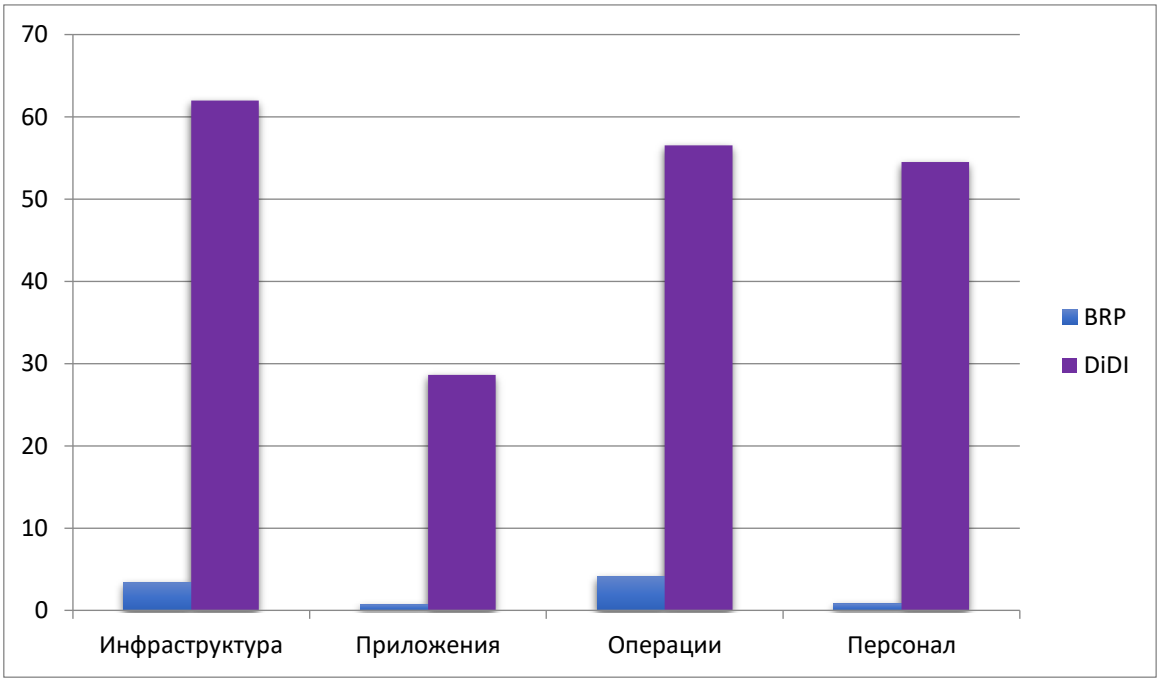

Рис. 7.1. Профиль риска для бизнеса и индекс эшелонированной защиты

Профиль риска для бизнеса – величина измерения риска, которому подвергается организация, в зависимости от бизнес-среды и отрасли, в условиях которых она конкурирует.

Области анализа: инфраструктура, приложения, операции и люди.

Индекс эшелонированной защиты (DiDI) – величина измерения защитных мер по обеспечению безопасности, используемых в отношении персонала, процессов и технологий для снижения рисков, выявленных на предприятии.

Интерпретация графиков. Показатель ПРБ находится в диапазоне от 0 до 100, где более высокая оценка подразумевает более высокий показатель потенциального риска для бизнеса в данной специфической области анализа. Важно отметить, что нулевое значение в данном случае невозможно, так как деловая деятельность сама по себе подразумевает наличие какого-либо уровня риска. Кроме того, важно понимать, что существуют определенные аспекты ведения бизнеса, для которых отсутствует прямая стратегия снижения риска.

Индекс DiDI также находится в диапазоне от 0 до 100. Высокий показатель свидетельствует о среде, в которой было принято множество мер для развертывания стратегий эшелонированной защиты (DiD) в конкретной области (AoA). Показатель DiDI не отражает общей эффективности безопасности или же ресурсы, затраченные на безопасность. Это скорее отражение общей стратегии, использованной для защиты среды.

На первый взгляд может показаться, что низкий показатель ПРБ и высокий показатель DiDI – это хороший результат, но это не всегда так. Масштаб данной самооценки не предусматривает все факторы, которые следует принять во внимание. При значительной диспропорции между показателями ПРБ и DiDI в конкретной области анализа рекомендуется изучить AoA как можно глубже. При анализе результатов важно учитывать соотношение индивидуальных показателей как для ПРБ, так и для DiDI. Стабильная среда, вероятно, будет представлена сравнительно одинаковыми показателями во всех областях. Разница между показателями DiDI – это явный признак того, что общая стратегия безопасности базируется на одной методике снижения риска. Если стратегия обеспечения безопасности не уравновешивает аспекты, связанные с персоналом, процессами и технологиями, то в среде существует вероятность повышенной уязвимости для злонамеренных атак.

Полный отчет. Введение. Средство MSAT для оценки риска, связанного с безопасностью, предназначено для оказания помощи в определении и устранении угроз безопасности в существующей вычислительной среде. В данном средстве реализован целостный подход к

оценке стратегии обеспечения безопасности с учетом персонала, процессов и технологий. Кроме полученных результатов, приводятся рекомендации по снижению риска, а также ссылки на дополнительную информацию, содержащую другие необходимые советы, которые могут помочь в получении дополнительных знаний о специальных средствах и методах, позволяющих повысить безопасность среды.

Полный отчет содержит итоговые сведения и предназначен для того, чтобы дать ИТ-менеджерам и высшему руководству представление о текущей ситуации с общей безопасностью в компании. Подробные результаты и рекомендации приводятся в детальном отчете.

Вводные данные – процесс и масштабы оценки. Оценка предназначена для выявления риска для бизнеса организации и определения мер безопасности, предпринимаемых для снижения риска. Сосредоточение внимания на общих проблемах этого сегмента рынка позволило разработать вопросы для обеспечения высококачественной оценки рисков, которые для ведения бизнеса представляют используемые технологии, процессы и персонал.

Профиль риска для бизнеса создается MSAT на основе серии предварительных вопросов о бизнес-модели компании. Тем самым измеряется риск для бизнеса, с которым компания сталкивается в данной отрасли и в условиях выбранной бизнес-модели. Прочие вопросы предлагаются с целью составления списка мер безопасности, которые со временем должны быть предприняты компанией. В целом эти меры безопасности формируют уровни защиты, обеспечивающие более серьезную защиту от угроз безопасности и конкретных уязвимых мест в системе. Каждый уровень способствует укреплению комбинированной стратегии эшелонированной защиты. В сумме это рассматривается как индекс эшелонированной защиты (DiDI). Затем ПРБ и DiDI сравниваются для измерения распределения риска по всем областям анализа – инфраструктуре, приложениям, операциям, персоналу.

Кроме измерения соотношения угрозы безопасности и методов защиты, MSAT также измеряет уровень безопасности организации. Последний подразумевает развитие высокоэффективных и стабильных методик обеспечения безопасности.

Уровень безопасности – это величина измерения способностей организации к эффективному использованию инструментов, доступных для создания стабильного уровня безопасности по многим дисциплинам.

При низком значении этого показателя используется ограниченное число методов защиты, а действия предпринимаются постфактум. При высоком значении практикуются устоявшиеся и проверенные процессы, которые позволяют компании предпринимать упреждающие меры и при необходимости реагировать еще эффективнее и согласованнее.

Для конкретной среды предлагаются рекомендации по управлению рисками, учитывающие уже развернутые технологии, текущее состояние безопасности и стратегии эшелонированной защиты. Выработанные предложения предназначены для того, чтобы помочь перейти к общепризнанным передовым методикам.

Данная оценка, включающая в себя вопросы, меры и рекомендации, предназначена для средних предприятий (организаций), в среде которых насчитывается от 50 до 500 настольных компьютеров. Она предполагает обширную защиту областей потенциального риска во всей среде, а не проведение углубленного анализа конкретной технологии или процесса. Таким образом, MSAT не рассчитано на измерение эффективности используемых мер безопасности. Отчет MSAT следует использовать как предварительное руководство, позволяющее сосредоточить внимание на определенных областях, требующих более пристального изучения. Он не должен заменять оценки в специфических областях, предлагаемые компетентными сторонними группами оценки.

Ситуационный анализ. В этом разделе, согласно представленным ответам, в графическом виде приведены концепции для организации (табл. 7.1).

Таблица 7.1

Результаты ситуационного анализа

Область анализа	Сравнение риска и защиты	Уровень безопасности
Инфраструктура	□	□
Приложения	□	□
Операции	□	□
Персонал	□	□

Risk-Defense. Диаграмма (рис. 7.2) отображает разность показателей эшелонированной защиты, упорядоченных по областям анализа.

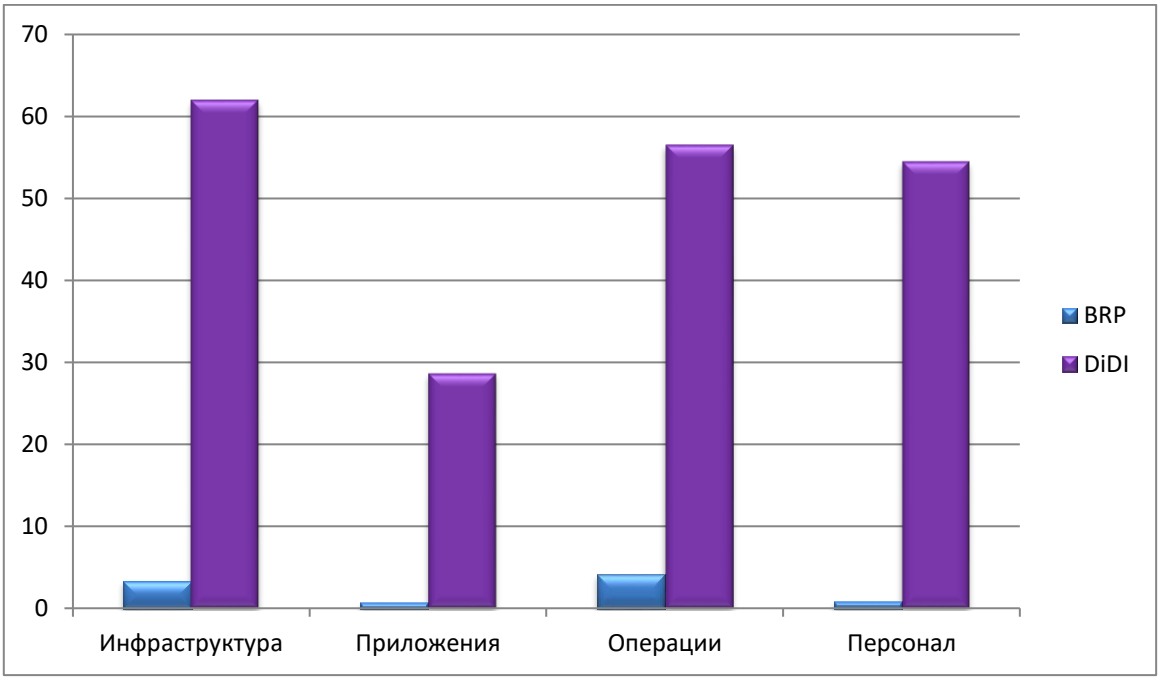

Рис. 7.2. Разность показателей эшелонированной защиты

Для одной и той же категории лучше всего иметь и рейтинг DiDI, и рейтинг ПРБ. Дисбаланс внутри одной категории или между разными категориями – в любом направлении – может означать необходимость перегруппировки инвестиций в ИТ.

Уровень безопасности. Включает в себя элементы управления (как физические, так и технические), техническую интуицию ИТ-ресурсов, политику, процесс и стабильные методики. Для определения областей, на которые должны быть нацелены программы безопасности организации, необходимо установить и применить базис уровня безопасности. Не все организации могут достичь оптимального уровня, однако все они должны оценить, на каком уровне они находятся и на каком должны находиться, учитывая существующий риск для бизнеса. Например, компании, осуществляющей деятельность в среде с низким риском, усовершенствования, находящиеся выше верхнего предела уровня «Базис» или ниже нижнего предела уровня «Стандарт», могут никогда не потребоваться. Компании же, осуществляющей деятельность в среде с высоким риском, возможно, потребуется выйти на уровень «Оптимизация». Показатели профиля риска для бизнеса помогают оценить уровень риска:

– *уровень безопасности* – величина, позволяющая сравнить методики, используемые компанией, с передовыми отраслевыми методиками с точки зрения стабильного уровня безопасности. Каждая компания должна стремиться к тому, чтобы ее уровень безопасности и связанная с ним стратегия безопасности соответствовали рискам, возникающим в процессе ведения бизнеса;

– *базис* – в качестве первичного механизма защиты применены некоторые упреждающие меры безопасности; в текущей деятельности и при реагировании на происшествия меры предпринимаются постфактум;

– *стандарт* – в соответствии с определенной стратегией развернуто несколько уровней защиты;

– *оптимизация* – эффективная защита по правильным направлениям с использованием надлежащих мер и постоянное использование передовых методик.

В таблицах 7.2, 7.3 приводятся рейтинг защитных мер для рисков и приоритеты областей, требующих усовершенствования.

Таблица 7.2

Рейтинг защитных мер, применяемых для различных рисков

Инфраструктура	**Операции**
Защита по периметру	**Среда**
Правила и фильтры межсетевого экрана	Узел управления
Антивирус	Узел управления – Серверы
Антивирус – Настольные компьютеры	Узел управления – Сетевые устройства
Антивирус – Серверы	**Политика безопасности**
Удаленный доступ	Классификация данных
Сегментация	Утилизация данных
Система определения вторжения (IDS)	Протоколы и службы
Беспроводная связь	Правильное использование
Проверка подлинности	Управление учетными записями
Административные пользователи	Управление
Внутренние пользователи	Политика безопасности
Пользователи с удаленным доступом	**Управление средствами исправления и обновления**
Политики паролей	Документация о сети
Политики паролей – Учетная запись администратора	Поток данных приложений
	Управление средствами исправления

Окончание табл. 7.2

Политики паролей – Учетная запись пользователя	Управление изменениями и конфигурация
Политики паролей – Учетная запись для удаленного доступа	**Архивация и восстановление**
Неактивные учетные записи	Файлы журнала
Управление и контроль	Планирование аварийного восстановления и возобновления деятельности предприятия
Нарушения безопасности: реагирование и создание отчетов	
Защищенная сборка	Архивация
Физическая безопасность	Резервные носители
Приложения	Архивация и восстановление
Развертывание и использование	**Персонал**
Балансировка нагрузки	**Требования и оценки**
Кластеризация	Требования по безопасности
Восстановление приложений и данных	Оценки безопасности
	Политика и процедуры
Независимый сторонний поставщик программного обеспечения	Проверка в фоновом режиме
	Политика отдела кадров
Внутренняя разработка	Сторонние взаимосвязи
Уязвимые места в системе	**Обучение и осведомленность**
Схема приложения	Осведомленность о безопасности
Проверка подлинности	
Политики паролей	Обучение в области безопасности
Авторизация и управление доступом	
Ведение журнала	
Подтверждение ввода	
Методологии разработки систем безопасности программного обеспечения	
Хранение данных и связь	
Шифрование	
Шифрование – Алгоритм	

Таблица 7.3

Приоритеты областей, требующих усовершенствования

Высокий приоритет	Средний приоритет	Низкий приоритет
Защищенная сборка Сегментация Сторонние взаимосвязи Независимый сторонний поставщик программного обеспечения Планирование аварийного восстановления и возобновления деятельности предприятия	Оценки безопасности Система определения вторжения (IDS) Классификация данных Утилизация данных Внутренняя разработка	Узел управления – Серверы Узел управления – Сетевые устройства Правильное использование Архивация Антивирус – Настольные компьютеры

Области анализа. В таблице 7.4 перечислены области, использованные для обеспечения высокого качества анализа при оценке угроз безопасности, и описана значимость каждой области для безопасности. В разделе «Подробная оценка» характеризуется состояние организации с точки зрения безопасности (исходя из предоставленных во время оценки ответов) в каждой из этих областей, а также приводятся признанные в отрасли передовые методики и рекомендации по их выполнению.

Таблица 7.4

Категории важности для обеспечения безопасности

Категория	**Важность для обеспечения безопасности**
Профиль риска для бизнеса	
Профиль риска для бизнеса	Понимание того, каким образом характер вашей деятельности оказывает влияние на риск, имеет огромное значение для определения тех областей, в которых следует применить ресурсы, чтобы ослабить угрозу безопасности. Распознавание критических областей риска для бизнеса поможет оптимизировать выделение средств на обеспечение безопасности
Инфраструктура	
Защита по периметру	Защита по периметру направлена на обеспечение безопасности на границах сети, где внутренняя сеть соединяется с внешним миром. Благодаря этому создается первая линия защиты от нежелательного вторжения

Продолжение табл. 7.4

Категория	**Важность для обеспечения безопасности**
Проверка подлинности	Строгие процедуры проверки подлинности для пользователей, администраторов и удаленных пользователей гарантируют невозможность получения несанкционированного доступа к сети с помощью локальных или удаленных атак
Управление и контроль	Управление, контроль и правильное ведение файлов журналов – важные условия для обслуживания и анализа среды ИТ. Важность этих инструментов еще более повышается после того, как имела место атака и требуется выполнить анализ происшествия
Приложения	
Развертывание и использование	При развертывании основных бизнес-приложений на производстве должна быть обеспечена как безопасность, так и доступность этих приложений и серверов. Непрерывное обслуживание имеет важное значение для своевременного создания исправлений, позволяющих устранить ошибки системы безопасности, и предотвращения появления новых проблем безопасности в среде
Схема приложения	Схема, которая неверно работает с такими механизмами обеспечения безопасности, как проверка подлинности, авторизация и проверка данных, помогает злоумышленникам воспользоваться уязвимыми местами в системе безопасности и тем самым получить доступ к конфиденциальной информации
Хранение данных и связь	Целостность и конфиденциальность данных – это одна из главных забот на любом предприятии. Потеря или кража данных может неблагоприятно сказаться на доходах организации и ее репутации. Важно понимать, каким образом приложения обрабатывают важные бизнес-данные и как эти данные защищены
Операции	
Среда	Безопасность организации зависит от эксплуатационных процедур, процессов и руководящих принципов, применяемых в среде. Они могут повысить безопасность организации благодаря тому, что представляют собой нечто большее, чем просто методы защиты технологий. Точная документация, относящаяся к среде, и правильные инструкции очень важны для группы по вопросам эксплуатации, так как они влияют на ее способность поддерживать и сохранять безопасность среды

Окончание табл. 7.4

Категория	Важность для обеспечения безопасности
Политика безопасности	Корпоративная политика безопасности связана с существующими индивидуальными политиками и инструкциями, которые позволяют управлять безопасным и надлежащим использованием технологии и процессов в организации. Эта область охватывает политики, направленные на обеспечение всех видов безопасности, относящихся к пользователю, системе и данным
Управление средствами исправления и обновления	Надлежащее управление исправлениями и обновлениями имеет важное значение для обеспечения безопасности в среде ИТ организации. Своевременное применение исправлений и обновлений – обязательное условие обеспечения защиты от известных проблем безопасности, которые могут быть использованы злоумышленниками
Архивация и восстановление	Архивация и восстановление данных – важная часть поддержки непрерывности ведения бизнеса в случае аварии или отказа аппаратного/программного обеспечения. Если в процедурах архивации и восстановления существуют ошибки или недостатки, они могут привести к значительным потерям данных и производительности
Персонал	
Требования и оценки	Все лица, принимающие решения, должны понимать требования по безопасности и следовать им, с тем чтобы их технические решения и бизнес-решения повышали безопасность, а не противоречили ей. Регулярно проводимые независимые оценки помогут компании рассмотреть, оценить и определить области, требующие улучшения
Политики и процедуры	Четкие практические процедуры для управления взаимосвязями с поставщиками и партнерами помогают ограничить подверженность компании риску. Процедуры, связанные с наймом сотрудников и их увольнением, помогают компании защититься от недобросовестных и недовольных сотрудников
Обучение и осведомленность	Необходимо проводить обучение сотрудников и разъяснять им важность обеспечения безопасности в повседневной работе, чтобы они не подвергали компанию всевозможным рискам

Оценочный анализ. Содержит четыре части, посвященные основным областям анализа, – инфраструктуре, приложениям, операциям и персоналу.

Инфраструктура. Под безопасностью инфраструктуры подразумевается то, каким образом должна функционировать сеть, какие бизнес-процессы (внутренние или внешние) она должна поддерживать, как создаются и развертываются узлы и как организовать управление сетью и ее обслуживание. Действенная безопасность инфраструктуры обеспечит значительные улучшения в областях сетевой защиты, реагирования на происшествия, сетевой доступности и анализа отказов. Создав надежную и понятную инфраструктуру и следуя ей, организация получает возможность определить области риска и разработать способы его снижения. Оценка предусматривает проверку процедур высокого уровня, которые организация может применять для снижения угрозы со стороны инфраструктуры, сосредоточившись на следующих областях безопасности, связанных с инфраструктурой:

– защита по периметру: межсетевые экраны, антивирусные программы, удаленный доступ, сегментация;

– проверка подлинности: политики паролей;

– управление и контроль: узлы управления, файлы журналов;

– рабочая станция: конфигурация сборки (табл. 7.5 – 7.10).

Таблица 7.5

Оценочный анализ: защита по периметру

Подкатегория	**Передовые методики**
Правила и фильтры межсетевого экрана	Брандмауэры представляют собой первый уровень защиты и должны размещаться на всех точках границ сетей. Применяемые на брандмауэрах правила должны отличаться высокой степенью ограничений и устанавливаться по принципу «узел – узел» и «служба – служба». При создании правил брандмауэра и списков ACL (списки управления доступом) маршрутизатора следует уделить особое внимание защите устройств управления доступом и сети от атак. Брандмауэр должен быть по умолчанию настроен на запрет любого трафика, за исключением необходимого. * Организуйте поток данных с помощью сетевых ACL и правил брандмауэра. * Протестируйте правила брандмауэра и списки ACL маршрутизатора, чтобы определить, достаточно ли существующих правил для предотвращения атак типа «отказ в обслуживании» (DoS). * Разверните одну или несколько демилитаризованных зон (DMZ) в качестве систематического и формального расширения брандмауэра.

Продолжение табл. 7.5

	* Разместите в демилитаризованных зонах все серверы, доступ к которым осуществляется через Интернет. Ограничьте входящие и исходящие подключения от демилитаризованных зон	
Подкатегория	**Полученные данные**	**Рекомендации**
Правила и фильтры межсетевого экрана	Вы указали, что межсетевые экраны развернуты в каждом офисе	Продолжайте развертывать межсетевые экраны или другие элементы управления доступом на сетевом уровне в каждом офисе и регулярно проверяйте их правильную работу
	Ваши ответы указывают на то, что вы не только развернули межсетевые экраны на границах сети, но и приняли также дополнительные меры предосторожности, создав один сегмент или более демилитаризованной зоны для защиты ресурсов, доступных по Интернету	Регулярно проверяйте политику межсетевого экрана и удаляйте устаревшие или неподходящие правила. Введите правила проверки входного и выходного доступа и рассмотрите необходимость реализации выходных фильтров для предотвращения лишних исходящих подключений. Ограничьте прямой доступ внутренних пользователей к сегментам демилитаризованной зоны, так как маловероятно, что они будут работать с хост-компьютерами, находящимися в ДМЗ на постоянной основе. Ограничьте доступ из основной сети в сегмент ДМЗ только конкретными узлами или административными сетями
	Вы указали, что для защиты серверов используется программное обеспечение межсетевого экрана на хост-компьютере	Продолжайте устанавливать узловые межсетевые экраны на все серверы и рассмотрите необходимость использования этого программного обеспечения на всех настольных и переносных компьютерах в организации

Продолжение табл. 7.5

Правила и фильтры межсетевого экрана	Вы указали, что межсетевой экран, обеспечивающий должную производительность, проверяется нерегулярно	Введите практику регулярной проверки межсетевого экрана. Проверьте правильную работу межсетевого экрана по отношению не только к внешнему, но также и к внутреннему трафику
Подкатегория	**Передовые методики**	
Антивирус	Разверните антивирусное программное обеспечение во всей среде предприятия как на уровне сервера, так и на уровне настольных компьютеров. Разверните специализированные антивирусные решения для выполнения конкретных задач, например средства проверки файловых серверов, средства отслеживания содержимого, а также средства проверки отправляемых и загружаемых данных. Настройте антивирусное программное обеспечение на поиск вирусов, пытающихся как проникнуть в ИТ-среду предприятия, так и покинуть ее. Антивирусное программное обеспечение должно быть в первую очередь установлено на критически важных файловых серверах. Затем область действия антивирусных программ следует распространить на почту, базы данных и веб-серверы. Антивирусное программное обеспечение настольных и переносных компьютеров следует включить в устанавливаемый по умолчанию набор программ. При работе с сервером Microsoft Exchange следует использовать его дополнительные возможности по антивирусной защите и фильтрации содержимого на уровне почтовых ящиков	
Подкатегория	**Полученные данные**	**Рекомендации**
Антивирус – Настольные компьютеры	Ваш ответ указывает на то, что антивирусные решения развернуты на уровне настольного компьютера	Продолжайте использовать такую практику. Реализуйте политику, в соответствии с которой пользователям необходимо регулярно обновлять сигнатуры вирусов. Рассмотрите необходимость установки клиента антивирусной программы с использованием настроек для рабочей станции по умолчанию

Продолжение табл. 7.5

Антивирус – Серверы	Ваш ответ указывает на то, что у вас развернуты антивирусные решения на уровне сервера	Продолжайте использовать такую практику. Рассмотрите необходимость активного управления антивирусными клиентами на серверах с централизованной консоли управления с целью развертывания конфигурации и сигнатур. Если используется Microsoft Exchange, рассмотрите необходимость активизации дополнительных антивирусных функций и функции фильтров содержимого на уровне почтового ящика
Подкатегория	**Передовые методики**	
Удаленный доступ	В целях обеспечения единообразия при проверке и оценке проблем и нарушений важно строго следовать задокументированным процедурам создания отчетов и реагирования на эти проблемы и нарушения. Важно, чтобы все пользователи осознавали свою ответственность за своевременное сообщение о любых нарушениях или проблемах, связанных с безопасностью. Поэтому необходимо иметь четко определенный процесс создания отчетов о подобных проблемах	
Сегментация	Сегментация используется для отделения определенных внешних сетей от доступа поставщика, партнера и клиента. В каждом сегменте внешней сети должна быть разрешена передача трафика только определенного приложения на определенные узлы и порты, которые используются для предоставления услуг клиентам. Следует убедиться, что сетевые элементы управления разрешают доступ только тем службам, которые требуются для каждого стороннего подключения. Необходимо ограничить доступ к сетевым службам на входе и выходе, а также между разными сетевыми сегментами	
Подкатегория	**Полученные данные**	**Рекомендации**
Сегментация	Ваш ответ указывает на то, что в сети вашей организации размещены службы, связанные с Интернетом	Убедитесь в наличии межсетевого экрана, сегментирования и систем определения вторжения для защиты инфраструктуры компании от атак из Интернета

Продолжение табл. 7.5

Сегментация	Вы указали, что в сети имеется более одного сегмента	Продолжайте использовать сегментацию сети для оптимизации управления сетевым трафиком и ограничения доступа к ресурсам в зависимости от требований к пользователям
	Ваш ответ указывает на то, что в вашей среде в настоящее время не используется сегментация сети. Важно сохранять службы внешней сети, относящиеся к клиентам/партнерам, в их собственных сегментах сети	Переместите серверы доступа к внешним сетям в физически отдельный сегмент сети. Используйте ограничительные элементы управления доступом, допускающие сторонний доступ только к определенным узлам, ограничьте доступ, сделав его возможным только к необходимым элементам корпоративной инфраструктуры, и заблокируйте попытки подключения к удаленным сетям
Подкатегория	**Передовые методики**	
Система определения вторжения (IDS)	Сетевые и узловые системы определения вторжения необходимо разворачивать для определения и уведомления об атаках корпоративных систем	
Подкатегория	**Полученные данные**	**Рекомендации**
Система определения вторжения (IDS)	Вы указали, что у вас используется сетевая система определения вторжения (NIDS)	Продолжайте практику развертывания сетевой системы определения вторжения. Следите за регулярным обновлением сигнатур вирусов, а также изучайте технологии предотвращения вторжения
	Вы указали, что у вас не используется узловая система определения вторжения (HIDS)	Рассмотрите необходимость развертывания узловых систем определения вторжения для оповещения администраторов об атаках, предпринятых против узлов, чтобы они могли своевременно реагировать на них

Окончание табл. 7.5

Подкатегория	**Передовые методики**	
Беспроводная связь	Передовые методики для беспроводной реализации должны гарантировать невыполнение сетью широковещательной рассылки SSID, использование WPA-шифрования и признание сети как незаслуживающей доверия	
Подкатегория	**Полученные данные**	**Рекомендации**
Беспроводная связь	Вы указали, что возможность беспроводного подключения к сети отсутствует	Если запретить используемый в данный момент беспроводной доступ, подверженность риску снижается. Однако если беспроводная связь планируется или будет реализована в будущем, реализация должна предусматривать отмену передачи идентификатора SSID, шифрование WPA и определение доверительных отношений в сети

Таблица 7.6

Оценочный анализ: защита по периметру – ресурсы

Программная среда	Характеристика	Адрес в Интернете
Windows Server 2008	Windows Server 2008 – это самая безопасная версия Windows Server. Операционная система была усилена для защиты от сбоев, а несколько новых технологий помогают предотвратить несанкционированные подключения к вашим сетям, серверам, данным и учетным записям пользователей. Защита доступа к сети (NAP) помогает гарантировать, что компьютеры, пытающиеся подключиться к вашей сети, соответствуют политике безопасности вашей организации. Технологическая интеграция и несколько улучшений делают службы Active Directory (AD) мощным унифицированным и интегрированным решением для идентификации и доступа (IDA), а контроллер домена только для чтения (RODC) и шифрование диска BitLocker позволяют более безопасно развертывать базу данных AD в филиалах	http://www.microsoft.com/windowsserver2008/en/us/overview.aspx

Окончание табл. 7.6

Программная среда	Характеристика	Адрес в Интернете
Internet Security and Acceleration Server	Internet Security and Acceleration (ISA) Server 2006 – это интегрированный пограничный шлюз безопасности, который помогает защитить ИТ-среду от интернет-угроз, предоставляя пользователям быстрый и безопасный удаленный доступ к приложениям и данным	http://www.microsoft.com/forefront/edgesecurity/default.mspx
Intelligent Application Gateway	Intelligent Application Gateway (IAG) 2007 от Microsoft – это комплексный безопасный шлюз удаленного доступа, который обеспечивает доступ и защиту приложений на основе защищенного уровня сокетов (SSL) с управлением безопасностью конечных точек. IAG 2007 обеспечивает детальное управление доступом, авторизацию и глубокую проверку контента с широкого спектра устройств и местоположений, а также с самых разных бизнес-ресурсов, интрасети и клиент-серверных ресурсов	http://www.microsoft.com/forefront/edgesecurity/iag/default.mspx
Network Access Protection	Защита доступа к сети (NAP) – это новая платформа и решение, которое контролирует доступ к сетевым ресурсам на основе удостоверения клиентского компьютера и соответствия политике корпоративного управления. NAP позволяет сетевым администраторам определять детальные уровни доступа к сети в зависимости от того, кем является клиент, к каким группам он принадлежит и насколько этот клиент соответствует политике корпоративного управления. Если клиент не соответствует требованиям, NAP предоставляет механизм для автоматического восстановления соответствия клиента требованиям, а затем динамически повышает уровень доступа к сети	http://technet.microsoft.com/en-us/network/bb545879.aspx

Таблица 7.7

Оценочный анализ: проверка подлинности

Подкатегория	**Передовые методики**	
Административные пользователи	Для администраторских учетных записей следует реализовывать строгую политику, требующую использования сложных паролей, отвечающих следующим требованиям: * алфавитно-цифровые * строчные и прописные буквы * хотя бы один специальный символ * минимальная длина – 14 символов Чтобы еще более снизить риск взлома пароля, выполните следующие рекомендации по контролю: * истечения срока действия пароля * блокировки учетной записи после 7 – 10 попыток неправильного ввода пароля * ведения журнала системы Кроме использования сложных паролей, следует также реализовать многофакторную проверку подлинности, обеспечить расширенный контроль над управлением учетными записями (запретить общие учетные записи), а также вести журнал доступа к учетной записи	
Подкатегория	**Полученные данные**	**Рекомендации**
Административные пользователи	Вы указали, что для административного доступа к управлению устройствами и хост-компьютерами необходима многофакторная проверка подлинности	Чтобы еще более снизить риск взлома пароля в административных учетных записях, выполните следующие рекомендации по контролю: * истечения срока действия пароля * блокировки учетной записи после 7 – 10 попыток неправильного ввода пароля * ведения журнала системы
	Вы указали, что в вашей среде для безопасного управления системами и устройствами используются индивидуальные имена для входа в систему	Продолжайте требовать введения различных учетных записей для административных/управленческих процессов и убедитесь, что учетные данные для группы администраторов меняются часто

Продолжение табл. 7.7

Административные пользователи	Вы указали, что пользователям не был предоставлен административный доступ к рабочим станциям	Продолжайте практику запрещения прав административного доступа конечных пользователей рабочих станций и убедитесь, что учетные данные для группы администраторов этих рабочих станций меняются часто
Подкатегория	**Передовые методики**	
Внутренние пользователи	Внедрите политику учетных записей пользователей, требующую использования сложных паролей, которые соответствуют следующим критериям: * буквенно-цифровые * с использованием нижнего и верхнего регистров * с использованием не менее одного специального символа * длиной не менее восьми символов Чтобы снизить вероятность атак с использованием пароля, введите следующие элементы управления: * истечение срока пароля * блокировку учетной записи после как минимум десяти неудачных попыток входа в систему * ведение системного журнала В дополнение к использованию сложных паролей рассмотрите возможность реализации многофакторной проверки подлинности. Реализуйте дополнительные элементы управления учетными записями (с запретом на совместное использование учетных записей) и ведение журнала доступа к учетным записям	
Подкатегория	**Полученные данные**	**Рекомендации**
Внутренние пользователи	Ваш ответ указывает на то, что в настоящее время для доступа пользователей к внутренней сети и хост-компьютерам необходима проверка подлинности только с использованием сложного пароля.	Рассмотрите необходимость внедрения дополнительного фактора проверки подлинности, который позволит существенно снизить риск несанкционированного доступа с использованием учетной записи пользователя. Следует обеспечить расширенный контроль над управлением учетными записями, а также вести журнал доступа к учетной записи

Продолжение табл. 7.7

	Пароль считается сложным, если он соответствует следующим критериям: * используются буквы и цифры * строчные и прописные буквы * хотя бы один специальный символ * минимальная длина – восемь символов	
Подкатегория	**Передовые методики**	
Пользователи с удаленным доступом	Внедрите элементы управления на основе сложных паролей для всех пользователей удаленного доступа, независимо от того, предоставляется ли доступ через телефонную сеть или через виртуальную частную сеть (VPN). Пароль считается сложным, если соответствует следующим критериям: * буквенно-цифровой * с использованием нижнего и верхнего регистров; * с использованием не менее одного специального символа * длиной не менее восьми символов Реализуйте дополнительные меры проверки подлинности для учетных записей с разрешением на удаленный доступ. Реализуйте также дополни-тельные элементы управления учетными записями (с запретом на совместное использование учетных записей) и ведение журнала доступа к учетным записям. В случае использования удаленного доступа особенно важно защитить рабочую среду с помощью надежных методов управления учетными записями, продуманного ведения журналов и средств обнаружения нарушений безопасности. Чтобы снизить вероятность атак методом прямого перебора паролей, можно реализовать следующие меры защиты: * истечение срока пароля * блокировка учетной записи после 7 – 10 неудачных попыток входа в систему * ведение системного журнала Службы удаленного доступа также должны учитывать системы, которые будут использоваться для получения доступа к сети или узлам. Также необходимо учесть возможность реализации элементов управления для узлов, с которых разрешен удаленный доступ к сети	

Продолжение табл. 7.7

Подкатегория	**Полученные данные**	**Рекомендации**
Пользователи с удаленным доступом	Ваши ответы показали, что в настоящее время проверка подлинности, необходимая для удаленного доступа пользователей к внутренней сети и хост-компьютерам, либо отсутствует, либо существует, но только с использованием простого пароля	Рассмотрите необходимость реализации элементов управления, предусматривающих наличие сложных паролей для всех пользователей с удаленным доступом, независимо от того, обеспечивается ли этот доступ с помощью технологий удаленного доступа или с помощью VPN. Пароль считается сложным, если он соответствует следующим критериям: * алфавитно-цифровой * строчные и прописные буквы * хотя бы один специальный символ * минимальная длина – восемь символов
Подкатегория	**Передовые методики**	
Политики паролей	Использование сложных паролей для всех учетных записей – ключевой элемент эшелонированной защиты. Сложные пароли должны быть длиной от 8 до 14 символов и содержать буквы, цифры и специальные символы. Для обеспечения дополнительной защиты необходимо задать минимальную длину, ведение хронологии журнала, длительность, а также преждевременное истечение срока действия паролей. Обычно срок истечения действия пароля должен задаваться следующим образом: * максимальная продолжительность – 90 дней * новые учетные записи должны изменять пароль при входе в систему * восемь паролей в журнале паролей (минимум восемь дней) Кроме использования сложных паролей, рекомендуется многофакторная проверка подлинности (особенно для учетных записей администратора и удаленного пользователя). Для всех учетных записей пользователей необходимо включить блокировку учетной записи после десяти неудачных попыток ввода пароля. Контроль блокировки учетной записи может варьироваться от простой	

Продолжение табл. 7.7

	блокировки в случае взлома пароля до необходимости вмешательства администратора для разблокировки учетной записи. Настоятельно рекомендуется включить блокировку учетных записей администраторов (хотя бы для сетевого доступа). При этом учетная запись будет блокироваться не на консоли, а только из сети. Возможно, это устроит не все организации, особенно те, которые имеют удаленные офисы. Для учетной записи удаленного доступа рекомендуется разблокировка учетной записи администратором, так как атаки могут оставаться незамеченными в течение значительного времени, если для отслеживания сбоев при проверке подлинности не используются другие средства. Рекомендуется выполнить следующие инструкции при реализации контроля блокировки учетной записи: * блокировка после 7 – 10 неудачных попыток ввода пароля для учетных записей администратора и удаленного доступа * блокировка после как минимум 10 неудачных попыток ввода пароля для обычных учетных записей пользователей * доступ с правами администратора для разблокировки учетных записей администратора и удаленного доступа, а также автоматическая разблокировка обычных учетных записей пользователей через пять минут Обычно ограничения по созданию паролей для администраторов должны быть еще более строгими, чем для обычных учетных записей. В системах Windows учетные записи администраторов (и учетные записи служб) должны задаваться с паролями длиной 14 символов, содержащими буквы, цифры и специальные символы	
Подкатегория	**Полученные данные**	**Рекомендации**
Политики паролей – Учетная запись администратора	Вы указали, что для учетных записей администратора реализованы политики паролей	Рассмотрите необходимость реализации дополнительной системы защиты, связанной с учетными записями администратора, например службы ведения журналов и учета всех успешных и неудачных попыток проверки подлинности. Перейдите с протоколов незашифрованного текста

Продолжение табл. 7.7

Подкатегория	**Полученные данные**	**Рекомендации**
Политики паролей – Учетная запись пользователя	Вы указали, что для учетных записей пользователей реализованы политики паролей	Рассмотрите необходимость реализации пороговых значений для неудачных попыток проверки подлинности при входе, чтобы системным администраторам посылались соответствующие сигналы. Рассмотрите необходимость тестирования политик паролей на месте
Политики паролей – Учетная запись для удаленного доступа	Вы указали, что для учетных записей удаленного доступа не реализованы политики паролей	Рассмотрите необходимость реализации политик паролей для учетных записей удаленного доступа на основе перечисленных передовых методик
Подкатегория	**Передовые методики**	
Неактивные учетные записи	Продолжайте наблюдать за неактивными учетными записями и управлять ими. Разработайте процедуру срочного уведомления всех системных администраторов об уволенных сотрудниках для немедленного отключения их учетных записей (особенно это касается учетных записей с возможностью удаленного доступа). Рассмотрите необходимость проверки текущих учетных записей сотрудников, переводимых в другие отделы внутри организации. Проверьте открытые компоненты вместе с ИТ-специалистами своей компании или деловым партнером по обеспечению безопасности. Чтобы получить более подробные сведения, введите наиболее подходящий ответ на вопрос в средстве MSAT. Следует регулярно посещать узлы соответствующего поставщика для получения обновлений сигнатур вирусов и загрузки обновлений в область карантина для проверки в лабораторных условиях. Перед развертыванием обновлений необходимо убедиться, что они не вызывают конфликты с развернутыми операционными системами или приложениями.	

Продолжение табл. 7.7

	Возможности автоматического обновления для антивирусных решений необходимо отключить во всех системах, чтобы предотвратить возможное повреждение файлов при их развертывании до проверки. Для антивирусных приложений рекомендуется развернуть центральную консоль, на которой можно будет просмотреть отчеты по устаревшим системам или отключенным программам. При наличии удаленных пользователей, которые редко подключаются к корпоративной сети, рекомендуется использовать функцию автообновления. Во избежание несанкционированного доступа к данным со стороны уволенного сотрудника или другого пользователя, использующего учетную запись уволенного сотрудника, данные учетные записи должны своевременно отключаться. Если системные администраторы не осведомлены об изменении статуса пользователя (например, при переводе пользователя в другой отдел), они не смогут своевременно повлиять на возможность доступа пользователя к системе или на возможность физического доступа. Такая ситуация может привести к несанкционированному доступу или доступу с повышенными правами таких сотрудников к данным	
Подкатегория	**Полученные данные**	**Рекомендации**
Неактивные учетные записи	Ответ указывает на то, что в организации используется формальный процесс проверки неактивных учетных записей пользователей	Продолжайте наблюдать за неактивными учетными записями и управлять ими
	Ваш ответ указывает на то, что в вашей среде все же существуют политики для обновления базы известных вирусов	Регулярно просматривайте узлы поставщиков и систем безопасности для ознакомления с предупреждениями о недавних атаках и появлении новых вирусов. Регулярно выполняйте аудит удаленных пользователей, чтобы проверить, выполняют ли они обновление своих систем.

Окончание табл. 7.7

Неактивные учетные записи		Постоянно выполняйте необходимые процедуры, используя перечисленные передовые методики
	Ответ указывает на то, что в организации отсутствует формальный процесс проверки неактивных учетных записей пользователей	Разработайте процедуру срочного уведомления всех системных администраторов об уволенных сотрудниках для немедленного отключения их учетных записей (особенно это касается учетных записей с возможностью удаленного доступа). Рассмотрите необходимость проверки текущих учетных записей сотрудников, переводимых в другие отделы внутри организации
	Вы указали, что не знаете ответа на этот вопрос	Проверьте открытые компоненты вместе с ИТ-специалистами своей компании или деловым партнером по обеспечению безопасности. Чтобы получить более подробные сведения, введите наиболее подходящий ответ на вопрос в средстве MSAT

Таблица 7.8

Оценочный анализ: проверка подлинности – ресурсы

Программная среда	Характеристика	Адрес в Интернете
Windows Server 2008	Windows Server 2008 – это самая безопасная версия Windows Server. Операционная система была усилена для защиты от сбоев, а несколько новых технологий помогают предотвратить несанкционированные подключения к вашим сетям, серверам, данным и учетным записям пользователей. Защита доступа к сети (NAP) помогает гарантировать, что компьютеры, пытающиеся подключиться к вашей сети, соответствуют политике безопасности вашей организации. Технологическая интеграция и несколько улучшений делают службы Active Directory мощным унифицированным и интегрированным решением для идентификации	http://www.microsoft.com/windowsserver2008/en/us/overview.aspx

Продолжение табл. 7.8

	и доступа (IDA), а контроллер домена только для чтения (RODC) и шифрование диска BitLocker позволяют более безопасно развертывать базу данных AD в филиалах	
Windows Server Active Directory	Служба каталогов Active Directory, центральный компонент платформы Windows, предоставляет средства для управления удостоверениями и отношениями, составляющими сетевые среды. Windows Server 2003 упрощает управление Active Directory, в частности миграцию и развертывание. Windows Server Active Directory уже используется компаниями по всему миру для унифицированного управления удостоверениями и ресурсами в корпоративной сети. Active Directory позволяет организациям централизованно управлять и отслеживать информацию о пользователях и их привилегиях. Кроме того, службы Active Directory облегченного доступа к каталогам (ADLDS), служба каталогов LDAP предоставляют организациям гибкую поддержку приложений и каталогов. Интеграция с решениями Microsoft Federated Identity, Strong Authentication, Information Protection и Identity Lifecycle Management делает Active Directory идеальной основой для создания комплексного решения для идентификации и доступа	http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx http://www.microsoft.com/windowsserver2003/technologies/idm/Directory-Services.mspx
Windows Server Group Policy	Групповая политика обеспечивает инфраструктуру для централизованного управления конфигурацией операционной системы и приложений, работающих в операционной системе. Групповая политика поддерживается как в Windows Server 2003, так и в Windows Server 2008, имеет функции для расширения возможностей текущей конфигурации	http://technet2.microsoft.com/windowsserver2008/en/library/3b4568bc-9d3c-4477-807d-2ea149ff06-491033.mspx?mfr=true
Windows Server 2003 – Internet Authentication Services (IAS)	Служба аутентификации в Интернете (IAS) – это реализация Microsoft сервером службы удаленной аутентификации пользователей (RADIUS) и прокси-сервера в Windows Server 2003. В качестве сервера RADIUS IAS выполняет централизованную аутентификацию подключений, авторизацию	http://technet.microsoft.com/en-us/network/bb643123.aspx

Продолжение табл. 7.8

Windows Server 2003 – Internet Authentication Services (IAS)	и учет для многих типов доступа к сети, включая беспроводные и виртуальные частные сети (VPN). В качестве прокси-сервера RADIUS IAS пересылает сообщения проверки подлинности и учета на другие серверы RADIUS. В Windows Server 2008 IAS был заменен сервером политики сети (NPS)	
Windows Server 2008 – Network Policy Server (NPS)	Сервер политики сети (NPS) – это реализация Microsoft сервером службы удаленной аутентификации пользователей (RADIUS) и прокси-сервера в Windows Server 2008. NPS – это замена службы аутентификации в Интернете (IAS) в Windows Server 2003. В качестве сервера RADIUS сервер политики сети выполняет централизованную проверку подлинности, авторизацию и учет для многих типов доступа к сети, включая подключения к беспроводной сети и виртуальной частной сети (VPN). В качестве прокси-сервера RADIUS сервер политики сети пересылает сообщения проверки подлинности и учета на другие серверы RADIUS. NPS также действует как сервер оценки работоспособности для защиты доступа к сети (NAP)	http://www.microsoft.com/windows/products/windowsvista/enterprise/benefits/operatingsystem.mspx?tab=Improve%20Security%20and%20Compliance
Public Key Infrastructure	Инфраструктура открытого ключа Microsoft (PKI) для Windows Server 2003 предоставляет интегрированную инфраструктуру открытого ключа, которая позволяет безопасно обмениваться информацией с надежной защитой и осуществлять простое администрирование через Интернет, экстрасети, интрасети и приложения	http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx
Certificates	Службы сертификатов Windows (CS) предоставляют интегрированную инфраструктуру открытых ключей, обеспечивающую безопасный обмен информацией. Благодаря высокой безопасности и простоте администрирования в Интернете, экстрасетях, интрасетях и приложениях CS предоставляет настраиваемые услуги для выпуска и управления сертификатами в системах безопасности программного обеспечения, использующих технологии открытого ключа	http://www.microsoft.com/windowsserver2003/technologies/idm/StrongAuthentication.mspx

Окончание табл. 7.8

Microsoft Identity Lifecycle Manager	Microsoft Identity Lifecycle Manager 2007 (ILM 2007) представляет собой интегрированное комплексное решение для управления всем жизненным циклом удостоверений пользователей и связанных с ними учетных данных. Он обеспечивает синхронизацию удостоверений, управление сертификатами и паролями, а также подготовку пользователей в едином решении, которое работает в Microsoft Windows и других операционных системах. В результате ИТ-организации могут определять и автоматизировать процессы, используемые для управления удостоверениями, от создания до вывода из эксплуатации	http://www.microsoft.com/windowsserver2003/technologies/idm/ILM.mspx

Таблица 7.9

Оценочный анализ: управление и контроль

Подкатегория	**Передовые методики**
Нарушения безопасности: реагирование и создание отчетов	Продолжайте следовать формальным процедурам реагирования на нарушения безопасности и предоставления отчетов. Разработайте и внедрите процедуры создания отчетов и реагирования на нарушения безопасности, а также на все проблемы, связанные с безопасностью. Назначьте группу быстрого реагирования, состоящую из представителей различных служб, включая технических специалистов, руководящих работников и юристов, чтобы обеспечить своевременное реагирование на все возможные проблемы, связанные с нарушением безопасности. Рассмотрите необходимость реализации комплексной программы реагирования на нарушения безопасности, включающей в себя создание групп быстрого реагирования, управление содержимым, анализ и процедуры реагирования на нарушения безопасности. Проверьте открытые компоненты вместе с ИТ-специалистами своей компании или деловым партнером по обеспечению безопасности. Чтобы получить более подробные сведения, введите наиболее подходящий ответ на вопрос в средстве MSAT.

Продолжение табл. 7.9

Нарушения безопасности: реагирование и создание отчетов	Планы аварийного восстановления и возобновления деятельности предприятия должны быть документально оформлены и соответствовать современным требованиям. Это позволит обеспечивать восстановление в приемлемые сроки. Планы (включая планы восстановления приложений из резервных копий) должны регулярно тестироваться на полноту и правильность. Планы непрерывной работы должны охватывать всю среду предприятия, включая ее физические и технологические составляющие, а также персонал. В целях обеспечения единообразия при проверке и оценке проблем и нарушений важно строго следовать задокументированным процедурам создания отчетов и реагирования на эти проблемы и нарушения. Важно, чтобы все пользователи осознавали свою ответственность за своевременное сообщение о любых нарушениях или проблемах, связанных с безопасностью. Поэтому необходимо иметь четко определенный процесс создания отчетов о подобных проблемах	
Подкатегория	**Полученные данные**	**Рекомендации**
Нарушения безопасности: реагирование и создание отчетов	Ваши ответы указывают на то, что в создаваемых рабочих станциях не используется формальный образ или документация	Создайте безопасный образ для каждого типа рабочей станции. Следует регулярно выполнять обновления, устанавливая последние пакеты обновления, исправления и другие меры безопасности
	Ответ указывает на то, что организация следует единообразным, формальным и документально закрепленным процессам реагирования на нарушения безопасности и предоставления отчетов	Продолжайте следовать формальным процедурам реагирования на нарушения безопасности и предоставления отчетов
	Ответ указывает на то, что организация не следует единообразным, формальным или документально закрепленным	Разработайте и внедрите процедуры создания отчетов и реагирования на нарушения безопасности, а также на все проблемы, связанные с безопасностью. Назначьте

Продолжение табл. 7.9

	процессам реагирования на нарушения безопасности и предоставления отчетов	группу быстрого реагирования, состоящую из представителей различных служб, включая технических специалистов, руководящих работников и юристов, чтобы обеспечить своевременное реагирование на все возможные проблемы, связанные с нарушением безопасности. Рассмотрите необходимость реализации комплексной программы реагирования на нарушения безопасности, включающей в себя создание групп быстрого реагирования, управление содержимым, анализ и процедуры реагирования на нарушения безопасности
Подкатегория	**Полученные данные**	**Рекомендации**
Защищенная сборка	Вы указали, что персональные межсетевые экраны установлены на всех рабочих станциях в среде	Рассмотрите необходимость развертывания сначала личных межсетевых экранов на всех мобильных переносных компьютерах. По умолчанию следует полностью заблокировать доступ к рабочей станции извне
	Вы указали, что процессы сборки для устройств инфраструктуры были документированы	Введите документирование процесса сборки для устройств инфраструктуры и обновляйте сборку при выпуске новых исправлений
	Вы указали, что клиентское программное обеспечение удаленного доступа не установлено на рабочих станциях, которые удаленно подсоединяются к корпоративным ресурсам	Если требуется удаленное подключение, рассмотрите необходимость развертывания клиентского программного обеспечения для удаленного доступа на всех отдельных рабочих станциях. Настройте клиентское программное обеспечение в соответствии с политикой удаленного доступа к серверу

Продолжение табл. 7.9

Защищенная сборка	Вы указали, что процессы сборки для серверов были документированы	Введите документирование процесса сборки для серверов и обновляйте сборку при выпуске новых исправлений
	Вы указали, что в вашей среде не используется программное обеспечение шифрования данных на диске	Рассмотрите необходимость использования программного обеспечения шифрования данных на диске во избежание нарушения их безопасности в случае кражи компьютера
	Вы указали, что процессы сборки для рабочих станций и переносных компьютеров были документированы	Введите документирование процесса сборки для рабочих станций и переносных компьютеров и обновляйте сборку при выпуске новых исправлений
	Вы указали, что в вашей среде не используется программное обеспечение удаленного контроля/управления	Продолжайте практику отказа от использования программного обеспечения удаленного контроля/управления
	Вы указали, что в вашей среде используется экранная заставка с парольной защитой	Продолжайте практику обязательной установки на компьютеры всех пользователей экранной заставки с парольной защитой с коротким периодом ожидания
	Вы указали, что в вашей среде не используются модемы	Продолжайте практику отказа от использования удаленного доступа через модем или телефонную сеть для снижения риска прямого подключения к компьютерам
Подкатегория	**Передовые методики**	
Физическая безопасность	Продолжайте реализовывать средства контроля физического доступа для обеспечения безопасности. Разработайте и внедрите средства контроля физического доступа для защиты от несанкционированного проникновения в офисное здание и получения доступа к конфиденциальным данным. Рассмотрите необходимость переоценки мер контроля физического доступа для определения их эффективности, а также степени их соблюдения.	

Продолжение табл. 7.9

	Повысьте осведомленность работников о политике контроля доступа персонала. Поощряйте уведомления о несанкционированном присутствии людей в офисном здании. Все компьютерные системы должны быть защищены от простых взломов. Необходимо поместить серверы и сетевые системы в запираемые корпуса и закрытые помещения с контролируемым доступом. Физический доступ необходимо строго контролировать с целью предотвращения несанкционированного доступа в офисные здания, к конфиденциальным данным и системам. Получив физический доступ, злоумышленник может изменить конфигурацию системы, нарушить безопасность сети и даже уничтожить или украсть оборудование	
Подкатегория	**Полученные данные**	**Рекомендации**
Физическая безопасность	Ваш ответ показал, что элементы управления физической безопасностью были развернуты для защиты имущества организации	Можно продолжить использование физических элементов управления, а также рассмотреть необходимость распространения их на все компьютерное оборудование, если этого еще не было сделано
	Вы указали, что система сигнализации была установлена для обнаружения незаконного вторжения и оповещения	Продолжите использование системы сигнализации. Периодически проверяйте ее (вместе с обслуживающей компанией), чтобы убедиться, что она работает правильно
	Ответ показывает, что все указанные меры или некоторые из них применяются. (идентификационные карточки для сотрудников и посетителей, сопровождение посетителей, журналы регистрации посетителей, контрольно-пропускные пункты)	Продолжайте реализовывать средства контроля физического доступа для обеспечения безопасности

Продолжение табл. 7.9

Физическая безопасность	Вы указали, что сетевое оборудование находится в закрытом помещении с ограниченным доступом	Продолжите практику защиты сетевого оборудования в запертой комнате и убедитесь, что доступ в нее имеют только те, кому это требуется по служебным обязанностям
	Ответ указывает на то, что идентификационные карточки для сотрудников и посетителей, сопровождение посетителей, журналы регистрации посетителей, контрольно-пропускные пункты не применяются	Разработайте и внедрите средства контроля физического доступа для защиты от несанкционированного проникновения в офисное здание и получения доступа к конфиденциальным данным. Рассмотрите необходимость переоценки мер контроля физического доступа для определения их эффективности, а также степени их соблюдения. Повысьте осведомленность работников о политике контроля доступа персонала. Поощряйте уведомления о несанкционированном присутствии людей в офисном здании
	Вы указали, что сетевое оборудование находится также в запираемом шкафу или стойке	Установка сетевого оборудования в запираемом шкафу или стойке обеспечивает дополнительную защиту от несанкционированного использования. Убедитесь, что доступ к клавишам и комбинациям имеют только те, кому это требуется по служебным обязанностям
	Ответ показывает, что все указанные меры или некоторые из них применяются (идентификационные карточки для сотрудников и посетителей, сопровождение	Продолжайте реализовывать средства контроля физического доступа для обеспечения безопасности

Продолжение табл. 7.9

	посетителей, журналы регистрации посетителей, контрольно-пропускные пункты)	
	Вы указали, что серверы находятся в закрытом помещении с ограниченным доступом	Продолжите практику защиты серверов в запертой комнате и убедитесь, что доступ в нее имеют только те, кому это требуется по служебным обязанностям
	Ответ указывает на то, что все указанные меры или некоторые из них применяются (идентификационные карточки для сотрудников и посетителей, сопровождение посетителей, журналы регистрации посетителей, контрольно-пропускные пункты)	Продолжайте реализовывать средства контроля физического доступа для обеспечения безопасности
	Вы указали, что серверы находятся также в запираемом шкафу или стойке	Установка серверов в запираемом шкафу или стойке обеспечивает дополнительную защиту от несанкционированного использования. Убедитесь, что доступ к клавишам и комбинациям имеют только те, кому это требуется по служебным обязанностям
	Вы указали, что рабочие станции не защищены кабельными замками	Чтобы предотвратить кражу, обеспечьте защиту рабочих станций с помощью кабельных замков
	Вы указали, что переносные компьютеры не защищены кабельными замками	Чтобы предотвратить кражу, обеспечьте защиту переносных компьютеров с помощью кабельных замков

Окончание табл. 7.9

Физическая безопасность	Вы указали, что конфиденциальные печатные материалы хранятся в запираемых картотечных шкафах	Продолжите практику хранения важных печатных материалов в запираемых картотечных шкафах. Кроме того, важные документы, которые больше не требуются, следует уничтожать

Таблица 7.10

Оценочный анализ: управление и контроль – ресурсы

Программная среда	Характеристика	Адрес в Интернете
Windows Server 2008	Windows Server 2008 – это самая безопасная версия Windows Server. Операционная система была усилена для защиты от сбоев, а несколько новых технологий помогают предотвратить несанкционированные подключения к вашим сетям, серверам, данным и учетным записям пользователей. Защита доступа к сети (NAP) помогает гарантировать, что компьютеры, пытающиеся подключиться к вашей сети, соответствуют политике безопасности вашей организации. Технологическая интеграция и несколько улучшений делают службы Active Directory мощным унифицированным и интегрированным решением для идентификации и доступа (IDA), а контроллер домена только для чтения (RODC) и шифрование диска BitLocker позволяют более безопасно развертывать базу данных AD в филиалах	http://www.microsoft.com/windowsserver2008/en/us/overview.aspx
Windows Server Active Directory	Служба каталогов Active Directory, центральный компонент платформы Windows, предоставляет средства для управления удостоверениями и отношениями, составляющими сетевые среды. Windows Server 2003 упрощает управление Active Directory, в частности миграцию и развертывание. Windows Server Active Directory уже используется компаниями по всему миру для унифицированного управления удостоверениями и ресурсами в корпоративной сети. Active Directory позволяет организациям централизованно управлять и отслеживать информацию о пользователях и их привилегиях. Кроме того, службы Active Directory облегченного доступа к каталогам (ADLDS),	http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx http://www.microsoft.com/windowsserver2003/technologies/idm/DirectoryServices.mspx

Продолжение табл. 7.10

Программная среда	Характеристика	Адрес в Интернете
	служба каталогов LDAP, предоставляют организациям гибкую поддержку приложений и каталогов. Интеграция с решениями Microsoft Federated Identity, Strong Authentication, Information Protection и Identity Lifecycle Management делает Active Directory идеальной основой для создания комплексного решения для идентификации и доступа	
Public Key Infrastructure	Инфраструктура открытого ключа Microsoft (PKI) для Windows Server 2003 предоставляет интегрированную инфраструктуру открытого ключа, которая позволяет вам безопасно обмениваться информацией и осуществлять простое администрирование через Интернет, экстрасети, интрасети и приложения	http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx
Certificates	Службы сертификатов Windows (CS) предоставляют интегрированную инфраструктуру открытых ключей, обеспечивающую безопасный обмен информацией. Благодаря высокой безопасности и простоте администрирования в Интернете, экстрасетях, интрасетях и приложениях CS предоставляет настраиваемые услуги для выпуска и управления сертификатами в системах безопасности программного обеспече-ния, использующих технологии открытого ключа	http://www.microsoft.com/windowsserver2003/technologies/idm/StrongAuthentication.mspx
Forefront Client Security	Forefront Client Security помогает защититься от новых угроз, таких как программы-шпионы и руткиты, а также от традиционных угроз, таких как вирусы, черви и троянские кони. Упрощая администрирование за счет централизованного управления и предоставляя критическую информацию об угрозах и уязвимостях, Forefront Client Security помогает вам надежно и эффективно защищать свой бизнес. Forefront Client Security интегрируется с существующим программным обеспечением инфраструктуры, таким как Microsoft Active Directory, и дополняет другие технологии безопасности Microsoft для повышения уровня защиты и контроля	http://www.microsoft.com/forefront/clientsecurity/en/us/overview.aspx

Продолжение табл. 7.10

Программная среда	Характеристика	Адрес в Интернете
Windows Vista – BitLocker Drive Encryption	Шифрование диска Bitlocker – это функция защиты данных, доступная в выпусках Windows Vista Enterprise и Ultimate, а также в Windows Server 2008. Bitlocker усиливает защиту данных, объединяя шифрование диска и проверку целостности компонентов ранней загрузки	http://www.microsoft.com/windows/products/windowsvista/features/details/bitlocker.mspx
Windows Vista – Encrypted File System (EFS)	Шифрованная файловая система (EFS) – это функция защиты данных в выпусках Business, Enterprise и Ultimate Windows Vista. EFS полезно для шифрования файлов и папок на уровне пользователя	http://www.microsoft.com/windows/products/windowsvista/features/details/encryptingfilesystem.mspx
Windows Vista and XPsp2 – Windows Defender	Защитник Windows работает с Internet Explorer 7, помогает сделать осознанный выбор при установке программного обеспечения на вашем ПК, обеспечивая постоянную защиту и мониторинг ключевых системных местоположений, отслеживая изменения, которые сигнализируют об установке и наличии шпионского ПО	http://www.microsoft.com/windows/products/windowsvista/features/details/defender.mspx
Windows Firewall	Брандмауэр Windows – это важнейшая первая линия обороны для защиты вашего компьютера от многих типов вредоносного программного обеспечения. Он может помочь остановить вредоносное ПО до того, как оно заразит ваш компьютер. Брандмауэр Windows входит в состав Windows Vista и включен по умолчанию для защиты вашей системы при запуске Windows	http://www.microsoft.com/windows/products/windowsvista/features/details/firewall.mspx
Windows Security Center	Центр обеспечения безопасности Windows предупреждает вас, когда ваше ПО для обеспечения безопасности устарело или необходимо усилить параметры безопасности. Он отображает настройки вашего брандмауэра и сообщает, настроен ли ваш компьютер для получения автоматических обновлений от Microsoft	http://www.microsoft.com/windows/products/windowsvista/features/details/securitycenter.mspx
Windows Live One Care	Защищайте, обслуживайте и управляйте своим компьютером с помощью Windows Live One Care – постоянно доступной службы по уходу за компьютером от Microsoft. Спокойно работая в фоновом режиме на вашем компьютере, One Care	http://onecare.live.com/standard/en-us/default.htm

Продолжение табл. 7.10

Программная среда	Характеристика	Адрес в Интернете
	защищает от вирусов, шпионских программ, хакеров и других нежелательных злоумышленников. Новые функции позволяют управлять несколькими ПК для формирования круга защиты, поддержки общего доступа к принтерам и централизованного резервного копирования до трех ПК, на которые распространяется одна и та же подписка One Care	
ISA Server	Internet Security and Acceleration (ISA) Server 2006 – это интегрированный пограничный шлюз безопасности, который помогает защитить ИТ-среду от интернет-угроз, предоставляя пользователям быстрый и безопасный удаленный доступ к приложениям и данным	http://www.microsoft.com/forefront/edge-security/iap.mspx http://www.microsoft.com/forefront/edgesecurity/sra. mspx
ADFS	Службы федерации Microsoft Active Directory (ADFS) обеспечивают взаимодействие, необходимое для упрощения широкого федеративного совместного использования цифровых удостоверений и политик за пределами организации. Беспрепятственно, но безопасно клиенты, партнеры, поставщики и мобильные сотрудники могут получить доступ к необходимой им информации, когда она им понадобится. ADFS повышает межорганизационную эффективность и совместную работу благодаря безопасному доступу к данным между компаниями, а также эффективность работы с помощью оптимизированных систем федерации и упрощенного управления идентификаторами и паролями. Это повышает прозрачность трансграничных процессов благодаря поддающимся аудиту правам и доступу к информации, а также повышает безопасность с помощью сопоставления утверждений ADFS, токенов SAML и проверки подлинности Kerberos. ADFS помогает снизить эксплуатационные расходы за счет использования существующих инвестиций в Active Directory и системы безопасности, а также устраняет сложность управления федерацией за счет использования Active Directory в качестве основного репозитория удостоверений	http://www.microsoft.com/windowsserver2003/technologies/idm/federatedidentity.mspx

Продолжение табл. 7.10

Программная среда	Характеристика	Адрес в Интернете
IPv6 Direct Connect	IPv6 предназначен для решения многих проблем пользователей версии IP (известной как IPv4), таких как исчерпание адресов, безопасность, автоконфигурация и расширяемость. Его использование также расширяет возможности Интернета и позволяет реализовать множество ценных и захватывающих приложений, включая одноранговые и мобильные приложения. Поддерживает новый интернет-протокол версии 6 (IPv6), набор стандартных протоколов для сетевого уровня Интернета, встроенный в последние версии Microsoft Windows, Windows Vista, Windows Server 2008, Windows Server 2003, Windows XP с пакетом обновления 2, Windows XP с пакетом обновления 1, Windows XP Embedded SP1 и Windows CE.NET	http://technet.microsoft.com/en-us/network/bb530961.aspx
IPSec	Безопасность интернет-протокола (IPSec) – это структура открытых стандартов для защиты связи в сетях интернет-протокола (IP) с помощью служб криптографической безопасности. IPSec поддерживает одноранговую аутентификацию на уровне сети, аутентификацию источника данных, целостность данных, конфиденциальность данных (шифрование) и защиту от воспроизведения. Реализация Microsoft IPsec основана на стандартах, разработанных рабочей группой IPSec. IPSec поддерживается операционными системами Microsoft Windows Vista, Windows Server 2008, Windows Server 2003, Windows XP и Windows 2000 и интегрирован со службой каталогов Active Directory. Политики IPSec можно назначать с помощью групповой политики, которая позволяет настраивать параметры IPSec на уровне домена, сайта или подразделения	http://technet.microsoft.com/en-us/network/bb531150.aspx

Окончание табл. 7.10

Программная среда	Характеристика	Адрес в Интернете
Стандарт IEEE 802.1X	Стандарт IEEE 802.1X для проводных сетей обеспечивает защиту аутентификации и авторизации на границе сети, где хост подключается к сети. IPSec обеспечивает сквозную аутентификацию одноранговых узлов и криптографическую защиту IP-трафика. В этом техническом документе описываются безопасность и возможности 802.1X для проводных сетей и IPSec на основе отраслевых стандартов и их поддержка в Windows Server 2003, Windows Server 2008, Windows XP и Windows Vista, а также предоставляется сравнительная информация при оценке развертывания этих технологий безопасности	http://technet2.microsoft.com/windowsserver/en/library/908d13e8-c4aa-4d62-8401-86d7da0eab481033.mspx?mfr=true

Приложения. Для полного изучения вопросов безопасности, касающихся приложений, требуются глубокие знания в области общей архитектуры приложений, а также абсолютное понимание пользовательской базы приложения. Только тогда можно приступать к определению потенциальных векторов угроз.

Учитывая ограниченный масштаб данной самооценки, полный анализ архитектуры приложений и всестороннее понимание пользовательской базы невозможны. Эта оценка предназначена для обзора приложений в организации и их градации с точки зрения безопасности и доступности. Для усовершенствования эшелонированной защиты выполняется проверка технологий, используемых в среде. Оценка предусматривает проверку процедур высокого уровня, которые организация может выполнять для снижения угрозы со стороны приложений, сосредоточившись на следующих областях безопасности, связанных с приложениями:

– развертывание и использование: механизмы повышения доступности;

– схема приложения: проверка подлинности, управление доступом, управление средствами обновления, проверка входных данных, ведение журнала и проверка;

– хранение данных и связь: шифрование, передача данных, ограничение доступа (табл. 7.11 – 7.14).

Таблица 7.11

Развертывание и использование: механизмы повышения доступности

Подкатегория	Полученные данные	Рекомендации
Балансировка нагрузки	Вы указали, что в вашей среде не развернуты средства выравнивания нагрузки	Рассмотрите необходимость развертывания аппаратных средств выравнивания нагрузки перед веб-серверами, чтобы обеспечить большую доступность. Подобное устройство позволяет увидеть из сети один (виртуальный) IP-адрес, который сопоставлен с адресами каждого веб-сервера в кластере
Кластеризация	Вы указали, что в среде не развернута кластеризация	Чтобы обеспечить высокую степень доступности для критически важных баз данных и хранилищ файлов, рассмотрите необходимость развертывания механизмов кластеризации
Восстановление приложений и данных	Вы указали, что в вашей организации отсутствуют важные бизнес-приложения	При отсутствии критически важного бизнес-приложения риск сбоя этих систем отсутствует. Однако, если в будущем планируется развертывание таких приложений, следует периодически проверять их безопасность, регулярно архивировать, полностью документировать и предусмотреть непредвиденные расходы, если эти меры не помогут
	Ваш ответ указывает на то, что регулярная проверка приложения и восстановление данных выполняются	Рассмотрите необходимость реализации политики хранения резервных носителей за пределами сети и политики периодического чередования этих носителей
Подкатегория	**Передовые методики**	
Независимый сторонний поставщик программного обеспечения	Сторонние независимые поставщики программного обеспечения должны регулярно предоставлять исправления и обновления собственных приложений, в которых должны содержаться сведения о назначении исправлений и их влиянии на функциональные возможности, конфигурацию или безопасность исправляемого приложения. Сторонние независимые поставщики программного	

Продолжение табл. 7.11

	обеспечения должны четко определить критические исправления для их немедленного применения. Сторонний независимый поставщик программного обеспечения должен объяснить все механизмы обеспечения безопасности приложения и предоставить последнюю версию документации. Организации должны быть известны все требования к конфигурации, необходимые для гарантии высочайшего уровня безопасности	
Подкатегория	**Полученные данные**	**Рекомендации**
Независимый сторонний поставщик программного обеспечения	Вы указали, что в вашей среде сторонние поставщики разработали одно или несколько основных приложений	Убедитесь, что сторонняя организация, которая разработала основное программное обеспечение, будет продолжать его поддержку, своевременно обеспечивать доставку обновлений и сможет предоставить исходный текст приложения в случае невозможности его дальнейшей поддержки
	Вы указали, что не знаете ответа на этот вопрос	Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на этот вопрос в средстве MSAT для получения дальнейших сведений
	Ваши ответы указывают на то, что сторонние независимые поставщики программного обеспечения (ISV) нерегулярно предоставляют вам программные обновления и исправления, повышающие безопасность приложений	Продолжите работу со сторонним поставщиком приложений для получения обновлений и исправлений как можно чаще и регулярнее. Когда появится исправление, прежде чем развертывать, тщательно проверьте его в лабораторных условиях. Получите от поставщика руководство по защите приложения, если таковое существует, и проверьте параметры настройки приложения
	Вы указали, что не знаете ответа на этот вопрос	Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на этот вопрос в средстве MSAT для получения дальнейших сведений

Продолжение табл. 7.11

Независимый сторонний поставщик программного обеспечения	Вы указали, что не знаете ответа на этот вопрос	Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на этот вопрос в средстве MSAT для получения дальнейших сведений
Подкатегория	**Передовые методики**	
Внутренняя разработка	Собственная группа разработки должна регулярно предоставлять исправления и обновления собственных приложений, в которых должны содержаться сведения о назначении исправлений и их влиянии на функциональные возможности, конфигурацию или безопасность исправляемого приложения. Группа разработки должна четко определить критические исправления для их немедленного применения. Группа разработки должна объяснить все механизмы обеспечения безопасности приложения и предоставить последнюю версию документации. Организации должны быть известны все требования к конфигурации, необходимые для гарантии высочайшего уровня безопасности. Рекомендуется заключить контракт с независимой сторонней фирмой на проверку архитектуры и развертывания приложения с целью определения всех проблем безопасности	
Подкатегория	**Полученные данные**	**Рекомендации**
Внутренняя разработка	Вы указали, что в вашей организации не используются специально разработанные макросы для офисных приложений	Постарайтесь по-прежнему не использовать собственные макросы Office, поскольку использование собственных макросов означает, что настройки безопасности пакета Office необходимо понизить, в результате чего офисные приложения могут быть подвержены заражению документами злоумышленников
Подкатегория	**Передовые методики**	
Уязвимые места в системе	Все известные проблемы системы безопасности должны быть определены и исправлены. Следует регулярно посещать веб-узлы поставщика и сторонних компаний, посвященные безопасности, для получения сведений о проблемах безопасности и имеющихся исправлениях. Если имеются известные проблемы системы безопасности,	

Окончание табл. 7.11

	для которых нет исправлений, следует выяснить, когда выйдет исправление, и разработать промежуточный план снижения рисков по этой проблеме. Рекомендуется обращаться к сторонней фирме для проведения периодических оценок системы безопасности приложения. Сторонняя оценка может также выявить области, где необходимы дополнительные механизмы обеспечения безопасности	
Подкатегория	**Полученные данные**	**Рекомендации**
Уязвимые места в системе	Ваш ответ указывает на то, что в настоящее время в любых приложениях, используемых в вашей среде, отсутствуют известные проблемы безопасности	Регулярно просматривайте узлы поставщиков и систем безопасности для ознакомления с возможными проблемами безопасности приложения. Можно подумать о том, чтобы провести независимую оценку схемы безопасности приложения при участии сторонних компаний с целью определения областей, где требуются дополнительные механизмы обеспечения безопасности

Таблица 7.12

Развертывание и использование:
механизмы повышения доступности – ресурсы

Программная среда	Характеристика	Адрес в Интернете
2007 Office Security Guide	По мере увеличения рисков злонамеренных атак механизмы безопасности настольных приложений развивались. Новая модель безопасности в выпуске Microsoft Office 2007 предоставляет новые механизмы, параметры и функции, которые позволяют вашей организации достичь эффективного баланса между защитой и производительностью при минимальном нарушении работы пользователей. Вы можете подумать, что такие риски исходят извне вашей организации и поэтому могут быть остановлены эффективными механизмами сетевой безопасности, такими как брандмауэры, прокси-серверы и системы обнаружения вторжений. Однако многие из этих бизнес-рисков могут исходить от внутренних пользователей и незащищенных систем,	http://www.microsoft.com/technet/security/guidance/client-security/2007office/default.mspx

Продолжение табл. 7.12

Программная среда	Характеристика	Адрес в Интернете
	лежащих в основе вашей организации. В отсутствие безопасной настройки настольные приложения, на которые полагаются ваши информационные работники при отправке электронной почты, написании документов, создании презентаций и анализе данных, могут быть важными путями для атак вредоносных программ, включая программы-шпионы, троянские кони, вирусы и черви	
Microsoft Rights Management Services for Windows Server 2003	Службы Microsoft Windows Rights Management Services (RMS) для Windows Server 2003 – это технология защиты информации, которая работает с приложениями, поддерживающими RMS, и помогает защитить цифровую информацию от несанкционированного использования как в сети, так и в автономном режиме, внутри и вне брандмауэра. RMS дополняет стратегию безопасности организации, защищая информацию с помощью постоянных политик использования, которые остаются с информацией, куда бы она ни направлялась. Организации могут использовать RMS для предотвращения преднамеренного или случайного попадания конфиденциальной информации, такой как финансовые отчеты, спецификации продуктов, данные о клиентах и конфиденциальные сообщения электронной почты, в чужие руки. Эти службы встроены в Windows Server 2008 как службы управления правами Active Directory (ADRMS)	http://www.microsoft.com/windowsserver2003/technologies/rights-mgmt/default.mspx
Windows Server 2008 – Active Directory Rights Management Services	Windows Server 2008, службы управления правами Active Directory (ADRMS) – это технология защиты информации, которая работает с приложениями с поддержкой ADRMS (Office 2007), помогая защитить цифровую информацию от несанкционированного использования. Владельцы контента могут определять, кто может открывать, изменять, печатать, пересылать или выполнять другие действия с информацией	http://technet2.microsoft.com/windowsserver2008/en/library/37c240d3-8928-4267-867b-4c005b72cca21033.mspx?mfr=true

Окончание табл. 7.12

Программная среда	Характеристика	Адрес в Интернете
Windows Server 2008 – Clustering	Отказоустойчивый кластер в Windows Server 2008 может помочь вам обеспечить избыточность вашей сети и устранить единые точки отказа. Усовершенствования отказоустойчивых кластеров (ранее известных как кластеры серверов) в Windows Server 2008 направлены на упрощение кластеров, повышение их безопасности и стабильности. Все это помогает сократить время простоя, защитить от потери данных и снизить общую стоимость владения. Поскольку они включены в выпуски Windows Server 2008 с расширенными возможностями, такие как Windows Server 2008 Enterprise и Windows Server 2008 Datacenter, отказоустойчивые кластеры Windows Server 2008 намного дешевле, чем сопоставимые системы, которые могут стоить тысячи долларов. Простота развертывания и доступность делают Windows Server 2008 идеальным решением высокой доступности для организаций любого размера	http://www.microsoft.com/windowsserver2008/en/us/clustering-home.aspx
Microsoft Security Development Lifecycle	Trustworthy Computing – это инициатива Microsoft, направленная на создание безопасного кода. Ключевой элемент инициативы Trustworthy Computing – жизненный цикл Microsoft Security Development Lifecycle (SDL). SDL – это инженерная практика, которая используется в сочетании со стандартными инженерными процессами для облегчения доставки безопасного кода. SDL состоит из десяти этапов, в ней сочетается передовой опыт с формализацией, измеримостью. Дополнительная структура включает в себя анализ дизайна безопасности, проверки качества на основе инструментов, тестирование на проникновение, окончательную проверку безопасности, управление безопасностью после выпуска продукта. Эта методология также доступна в виде книги через Microsoft Press	http://msdn.microsoft.com/en-us/library/aa969774.aspx

Таблица 7.13

Схема приложения

Подкатегория	**Передовые методики**	
Проверка подлинности	В приложении должен быть реализован способ проверки подлинности, надежность которого соответствует требованиям безопасности данных или доступа к функциям. В приложениях, зависящих от паролей, должны быть предусмотрены ограничения с точки зрения сложности пароля, включающие в себя сочетание букв, цифр и символов, минимальную длину, ведение журнала, длительность, преждевременное истечение срока действия и проверку по словарю. Приложение должно регистрировать безуспешные попытки входа в систему в обход пароля. Каждый компонент, предоставляющий доступ к данным или функциям, должен контролировать наличие правильных учетных данных для проверки подлинности. Административные права доступа к системам должны быть защищены самым надежным механизмом проверки подлинности. Обычно ограничения по созданию паролей для администраторов должны быть еще более строгими, чем для обычных учетных записей. Кроме использования сложных паролей с надежными политиками, для дополнительной безопасности рекомендуется использовать многофакторную проверку подлинности	
Подкатегория	**Полученные данные**	**Рекомендации**
Проверка подлинности	Ваш ответ указывает на то, что в настоящее время для основных приложений применяется метод проверки подлинности с использованием сложного пароля	Рассмотрите необходимость внедрения дополнительного фактора проверки подлинности (маркер, смарт-карта...) для важных внешних приложений. Кроме того, следует обеспечить расширенный контроль над управлением учетными записями, а также вести журнал доступа к учетной записи

Продолжение табл. 7.13

Подкатегория	**Передовые методики**	
Политики паролей	Использование сложных паролей – ключевой элемент эшелонированной защиты. Сложные пароли должны быть длиной от 8 до 14 символов и содержать буквы, цифры и специальные символы. Для обеспечения дополнительной защиты паролей необходимо настроить их минимальную длину, длительность, ведение хронологии журнала, а также преждевременное истечение срока действия паролей. Обычно срок истечения действия пароля должен задаваться следующим образом: * максимальная продолжительность – 90 дней * новые учетные записи должны изменять пароль при входе в систему * восемь паролей в журнале паролей (минимум восемь дней) Административные права доступа к системам должны быть защищены самым надежным механизмом проверки подлинности. Обычно ограничения по созданию паролей для администраторов должны быть еще более строгими, чем для обычных учетных записей. Если для обычных учетных записей длина пароля должна составлять восемь символов, то для учетных записей администраторов пароли должны быть длиной 14 символов. Для всех учетных записей пользователей необходимо включить блокировку учетной записи после 10 неудачных попыток ввода пароля. Контроль блокировки учетной записи может варьироваться от простой блокировки в случае взлома пароля до сложных случаев, требующих вмешательства администратора для разблокировки учетной записи. Рекомендуется выполнить следующие инструкции при реализации контроля блокировки учетной записи: * блокировка после как минимум 10 неудачных попыток ввода пароля для учетных записей пользователей * доступ с правами администратора для разблокировки учетных записей важных приложений, а также автоматическая разблокировка обычных учетных записей пользователя через пять минут для других приложений * промежуток в 30 минут для кэширования сбоев обычных учетных записей пользователя	
Подкатегория	**Полученные данные**	**Рекомендации**
Политики паролей	Ваш ответ указывает на то, что для основных приложений реализованы эффективные элементы управления, предусматривающие наличие паролей	Рассмотрите необходимость реализации пороговых значений для неудачных попыток проверки

Продолжение табл. 7.13

Политики паролей		подлинности при входе, чтобы системным администраторам посылались соответствующие сигналы. Кроме того, рассмотрите необходимость распространения надежных паролей на все приложения
	Ваш ответ указывает на то, что в основных приложениях реализован элемент управления истечением срока действия пароля	Рассмотрите необходимость распространения политики ограничения срока действия паролей на все внешние приложения и основные внутренние приложения
	Ваш ответ указывает на то, что в основных приложениях реализованы элементы управления блокировкой учетных записей	Рассмотрите необходимость распространения политики блокировки учетных записей на все внешние приложения и важные внутренние приложения
Подкатегория	**Передовые методики**	
Авторизация и управление доступом	В приложениях должен быть реализован механизм авторизации, который обеспечивает доступ к критическим данным и функциям только для пользователей и клиентов, имеющих соответствующие права. Управление доступом на основе ролей должно быть усилено на уровне базы данных и интерфейса приложения. Это обеспечит защиту базы данных в случае взлома клиентского приложения. Для успешной проверки подлинности необходимо пройти авторизацию. Все попытки получения доступа без авторизации должны регистрироваться в журнале. Следует проводить регулярные проверки основных приложений, которые обрабатывают критические данные, а также интерфейсов, доступных для пользователей из сети Интернет. Приложения следует проверять в режимах «черного ящика» и «подробного описания». Необходимо определить, имеют ли пользователи доступ к данным с других учетных записей	

Продолжение табл. 7.13

Подкатегория	**Полученные данные**	**Рекомендации**
Авторизация и управление доступом	Ваш ответ указывает на то, что основные приложения ограничивают доступ к критическим данным и функциональным возможностям, исходя из привилегий, назначенных учетной записи	Рассмотрите необходимость проведения целенаправленной проверки основных приложений, которые обрабатывают критические данные, а также интерфейсов, доступных для пользователей из сети Интернет. Приложения следует проверять в режимах «черного ящика» и «подробного описания»
Подкатегория	**Передовые методики**	
Ведение журнала	Ведение журнала должно быть включено для всех приложений в системе. Данные файла журнала важны для анализа происшествий и тенденций, а также для проверки. Приложение должно регистрировать все безуспешные и успешные попытки проверки подлинности, изменения данных приложения, включая учетные записи пользователей, неустранимые ошибки приложений, а также безуспешный и успешный доступ к ресурсам. При записи данных в файл журнала приложение не должно записывать конфиденциальные данные	
Подкатегория	**Полученные данные**	**Рекомендации**
Ведение журнала	Ваши ответы указывают на то, что в данной среде разные события регистрируются приложениями. Приложения должны заносить в журналы все события на основе перечисленных передовых методик	Для облегчения управления файлами журнала и их анализа рассмотрите необходимость интеграции с централизованным механизмом ведения журналов. Механизм ведения журналов должен обеспечивать сохранение и архивирование журналов в соответствии с действующими политиками хранения корпоративных данных
	Вы указали, что неудачные попытки проверки подлинности фиксируются в журнале	Продолжайте ведение журнала неудачных попыток проверки подлинности

Продолжение табл. 7.13

Ведение журнала	Вы указали, что успешные проверки подлинности не фиксируются в журнале	Рассмотрите необходимость ведения журнала успешных проверок подлинности для отслеживания активности пользователей
	Вы указали, что ошибки приложения не фиксируются в журнале	Рассмотрите необходимость ведения журнала ошибок приложений для получения возможности обнаружения и диагностики троянских коней
	Вы указали, что отказ в доступе к ресурсам фиксируется в журнале	Продолжайте ведение журнала отказов в доступе к ресурсам
	Вы указали, что успешный доступ к ресурсам не фиксируется в журнале	Рассмотрите необходимость ведения журнала успешного доступа к ресурсам для отслеживания поведения злоумышленника после свершившегося несанкционированного доступа
	Вы указали, что изменения в данных фиксируются в журнале	Продолжайте ведение журнала изменений данных
	Вы указали, что изменения в учетных записях пользователей фиксируются в журнале	Продолжайте ведение журнала изменений в учетных записях пользователей
Подкатегория	**Передовые методики**	
Подтверждение ввода	Приложение может принимать входные данные во многих точках от внешних источников, например пользователей, клиентских приложений, а также от систем передач данных. Оно должно проводить проверки вводимых данных на синтаксическую и семантическую достоверность. Это приложение также должно проверять, не нарушают ли вводимые данные ограничения базовых или зависимых компонентов, в частности по длине строки и набору символов. Все пользовательские поля должны проверяться на сервере	

Продолжение табл. 7.13

Подкатегория	**Полученные данные**	**Рекомендации**
Подтверждение ввода	Вы указали, что не знаете ответа на этот вопрос	Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на этот вопрос в средстве MSAT для получения дальнейших сведений
Подкатегория	**Передовые методики**	
Методологии разработки систем безопасности программного обеспечения	Продолжайте использовать методологии разработки систем безопасности программного обеспечения. Разработайте и внедрите методологии разработки систем безопасности программного обеспечения для повышения безопасности приложений. При сотрудничестве с консультантами или поставщиками на любом этапе цикла разработки убедитесь в том, что их персонал прошел обучение методологии разработки систем безопасности программного обеспечения, используемой или рекомендуемой к использованию в организации. Весь коллектив разработчиков организации должен пройти обучение по рекомендуемой методологии разработки систем безопасности программного обеспечения. Это касается руководителей отделов разработки, разработчиков, испытателей и специалистов по контролю качества. Учитывая постоянное развитие угроз безопасности, следует ежегодно обновлять программу обучения методологии разработки систем безопасности программного обеспечения и программу обучения моделированию угроз. Все разработчики должны ежегодно проходить обновленные курсы по разработке систем безопасности программного обеспечения. Применение средств тестирования программ для обеспечения безопасности расширяет возможности команды разработчиков по эффективному написанию безопасного кода. Результаты применения средств тестирования должны включаться в программу обязательного ежегодного обучения	

Окончание табл. 7.13

Подкатегория	Полученные данные	Рекомендации
Методологии разработки систем безопасности программного обеспечения	Ответ указывает на то, что организация использует средства тестирования программ для обеспечения безопасности в качестве части процесса разработки систем безопасности	Расширьте использование средств тестирования программ по обеспечению безопасности в качестве первостепенного средства реализации планов разработки систем безопасности
	Ответ указывает на то, что организация не обучает разработчиков методологии разработки систем безопасности программного обеспечения	Разработайте программу обучения методологии разработки систем безопасности программного обеспечения, чтобы усовершенствовать навыки сотрудников по созданию безопасного кода

Таблица 7.14

Хранение данных и связь

Подкатегория	Передовые методики
Шифрование	Критические данные должны быть зашифрованы или хешированы в базе данных и файловой системе. В приложении должно проводиться различие между критическими для раскрытия данными, которые необходимо шифровать, и данными, критическими только с точки зрения подделки, для которых необходимо генерировать введенное хеш-значение (HMAC), а также данными, которые могут быть безвозвратно преобразованы (хешированы) без потери функциональности (например, пароли). Ключи, использующиеся для дешифрации, должны храниться в приложении отдельно от зашифрованных данных. Критические данные должны шифроваться до передачи в другие компоненты. Следует проверить, что промежуточные компоненты, обрабатывающие данные в незашифрованной форме до передачи получателю, не представляют угрозы для данных. Приложение должно воспользоваться средствами проверки подлинности, доступными в рамках механизма обеспечения безопасности транспорта. Примеры широко используемых шифров следующие: 3DES, AES, RSA, RC4 и Blowfish. Рекомендуется использовать ключи не менее 128 бит (1024 бит для RSA)

Окончание табл. 7.14

Подкатегория	**Полученные данные**	**Рекомендации**
Шифрование	Вы указали, что не знаете ответа на этот вопрос	Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на этот вопрос в средстве MSAT для получения дальнейших сведений
Подкатегория	**Передовые методики**	
Шифрование – Алгоритм	В приложении должны использоваться стандартные для отрасли алгоритмы шифрования с ключами соответствующих размеров и необходимыми режимами шифрования. К признанным в отрасли шифрам относятся 3DES, AES, RSA, Blowfish и RC4. Необходимо использовать ключ размером не менее 128 бит (1024 бит для RSA)	

Операции. В этой области анализа исследуются методы, процедуры эксплуатации и рекомендации, которым следует организация, для усовершенствования эшелонированной защиты. Данная оценка предполагает проверку политик и процедур, управляющих сборками системы, сетевой документацией и использованием технологий в среде. Она также включает в себя поддержку функций, необходимых для управления информацией и процедурами, которые используются администраторами и оперативным персоналом в данной среде. Создав понятные рабочие методики, процедуры и рекомендации и следуя им, организация может потенциально улучшить состояние эшелонированной защиты. Оценка предусматривает проверку процедур высокого уровня, которые организация может выполнять для снижения угрозы со стороны операций, сосредоточившись на следующих областях безопасности, связанных с операциями:

– среда: сборка системы, сетевая документация, поток данных приложения, архитектура приложений;

– политика безопасности: протоколы и службы, правильное использование, управление учетными записями;

– управление средствами исправления и обновления: управление исправлениями, сигнатуры вирусов;

– архивация и восстановление: архивация, хранение, проверка (табл. 7.15 – 7.20).

Таблица 7.15

Среда

Подкатегория	**Передовые методики**	
Узел управления	При использовании пакетов управления следует позаботиться об усилении безопасности и физической защите консолей администрирования.Усильте безопасность рабочих станций, используемых для управления серверами сети и сетевыми устройствами. Защитите протоколы управления, использующие открытый текст, с помощью SSH или VPN-подключений. Рабочие станции управления должны быть выделены конкретным сетям и администраторам узлов. Протестируйте все системы управления, использующие SNMP, чтобы убедиться в том, что они обновлены до последних версий и не используют настройки сообщества по умолчанию. В системах общего пользования не должно храниться никаких данных, относящихся к управлению. Рабочие станции с совместным доступом не следует использовать для администрирования сетевых устройств или узлов	
Подкатегория	**Полученные данные**	**Рекомендации**
Узел управления – Серверы	Ваши ответы указывают на то, что для серверов существует выделенный управляющий компьютер	Рассмотрите необходимость использования SSH или VPN для защиты текстовых протоколов
Узел управления – Сетевые устройства	Вы указали, что развернули выделенный управляющий компьютер для управления сетевыми устройствами	Следует протестировать все системы управления, в которых используется SNMP, чтобы убедиться, что в них используются последние версии исправлений и не используются настройки сообщества по умолчанию

Таблица 7.16

Среда – ресурсы

Программная среда	Характеристика	Адрес в Интернете
Windows Vista – User Account Controls	Элементы управления учетными записями пользователей в Windows Vista повышают безопасность и защищенность вашего компьютера, предотвращая внесение изменений в ваш компьютер опасным программным обеспечением без вашего явного согласия. Они запрещают пользователям устанавливать мошеннические программы, изменять системные настройки и выполнять другие задачи, которые решаются системными администраторами	http://www.microsoft.com/windows/products/windowsvista/features/details/useraccountcontrol.mspx
Data Classification and Protection Whitepaper	Классификация и защита данных касается того, как применять уровни классификации безопасности к данным либо в системе, либо при передаче	http://www.microsoft.com/technet/security/guidance/complianceandpolicies/compliance/rcguide/411-00.mspx?mfr=true

Таблица 7.17

Политика безопасности

Подкатегория	**Передовые методики**
Классификация данных	Продолжайте реализовывать классификацию данных с соответствующими рекомендациями по защите. Определите схему классификации корпоративных данных и организуйте соответствующие инструктаж и обучение всего персонала. Определите требования к обработке и защите данных в соответствии с уровнями их классификации. Проверьте открытые компоненты вместе в ИТ-специалистами своей компании или деловым партнером по обеспечению безопасности. Чтобы получить более подробные сведения, введите наиболее подходящий ответ на вопрос в средстве MSAT (Microsoft Security Assessment Tool). Необходимо иметь схему классификации данных с соответствующими рекомендациями по их защите. Недостаточное разделение и классификация данных могут привести к тому, что конфиденциальные данные станут доступны персоналу, деловым партнерам или широкой общественности. Подобное

Продолжение табл. 7.17

Классификация данных	несанкционированное раскрытие конфиденциальных данных может нанести урон репутации торговой марки или поставить компанию в неловкое положение. Ограниченный объем ресурсов по защите данных может быть использован нерационально и не обеспечит их надлежащей классификации. Если персонал компании не осведомлен о том, какие данные конфиденциальные, а также о том, как следует их защищать, вероятность несанкционированного доступа к этим данным увеличивается	
Подкатегория	**Полученные данные**	**Рекомендации**
Классификация данных	Ответ указывает на то, что в организации применяются схема классификации данных и рекомендации по защите данных, разработанные на основе классификации	Продолжайте реализовывать классификацию данных с соответствующими рекомендациями по защите
	Ответ указывает на то, что в организации отсутствуют схема классификации данных или рекомендации по защите данных, разработанные на основе классификации	Определите схему классификации корпоративных данных и организуйте соответствующие инструктаж и обучение всего персонала. Определите требования к обработке и защите данных в соответствии с уровнями их классификации
	Вы указали, что не знаете ответа на этот вопрос	Проверьте открытые компоненты вместе с ИТ-специалистами своей компании или деловым партнером по обеспечению безопасности. Чтобы получить более подробные сведения, введите наиболее подходящий ответ на вопрос в средстве MSAT (Microsoft Security Assessment Tool)
Подкатегория	**Передовые методики**	
Утилизация данных	Продолжайте реализовывать процедуры удаления данных. Определите и внедрите процедуры управления данными и их утилизации как для бумажных копий, так и для данных в электронном виде (например, данных, хранящихся на дискетах и жестких дисках).	

Продолжение табл. 7.17

	Проверьте открытые компоненты вместе с ИТ-специалистами своей компании или деловым партнером по обеспечению безопасности. Чтобы получить более подробные сведения, введите наиболее подходящий ответ на вопрос в средстве MSAT (Microsoft Security Assessment Tool). Необходимо реализовать формальные процедуры, регламентирующие утилизацию пользователями данных как в бумажном, так и в электронном виде. В случае отсутствия рекомендаций и процедур безопасного уничтожения данных конфиденциальные сведения могут оказаться в опасности	
Подкатегория	**Полученные данные**	**Рекомендации**
Утилизация данных	Ответ указывает на то, что организация следует документально закрепленным процессам утилизации данных	Продолжайте реализовывать процедуры удаления данных
	Ответ указывает на то, что организация не следует документально закрепленным процессам утилизации данных	Определите и внедрите процедуры управления данными и их утилизации как для бумажных копий, так и для данных в электронном виде (например, данных, хранящихся на дискетах и жестких дисках)
	Вы указали, что не знаете ответа на этот вопрос	Проверьте открытые компоненты вместе с ИТ-специалистами своей компании или деловым партнером по обеспечению безопасности. Чтобы получить более подробные сведения, введите наиболее подходящий ответ на вопрос в средстве MSAT (Microsoft Security Assessment Tool)
Подкатегория	**Передовые методики**	
Протоколы и службы	Следует четко задокументировать стандарты и процедуры, чтобы отразить, какие протоколы и службы можно использовать в организации. Необходимо проверить списки управления доступом, чтобы убедиться, что уровень предоставленного доступа для всех разрешенных служб действительно необходим в компании. При возможности необходимо задать определенный IP-адрес/диапазон. На серверах должны быть установлены только те службы, которые необходимы для нужд компании. Кроме того, в инструкциях должны	

Продолжение табл. 7.17

Протоколы и службы	содержаться данные версии протокола и минимальной стойкости шифрования. Следует обеспечить более надежную защиту при использовании протокола за счет устройств внешнего доступа (маршрутизаторов, шлюзов, межсетевых экранов и т. д.), строгой проверки подлинности и шифрованных соединений	
Подкатегория	**Полученные данные**	**Рекомендации**
Протоколы и службы	Ваш ответ указывает на то, что у вас имеются документированные указания, которые предписывают, какие протоколы и службы разрешены в корпоративной сети	Проведите аудит документации, выясните, какие протоколы и службы разрешены, и убедитесь, что документация соответствует настроенным спискам управления доступом и правилам межсетевого экрана на соответствующих устройствах. Опубликуйте эти сведения в корпоративной интрасети и реализуйте политики, регулирующие внесение изменений в правила
Подкатегория	**Передовые методики**	
Правильное использование	Политика правильного использования предназначена для обеспечения надлежащего использования корпоративных сетей, приложений, данных и систем. Эта политика также должна регулировать данные мультимедиа, печатные носители и другую интеллектуальную собственность	
Подкатегория	**Полученные данные**	**Рекомендации**
Правильное использование	Ваш ответ указывает на то, что в вашей организации существует корпоративная политика правильного использования	Все сотрудники и клиенты должны быть ознакомлены с этими политиками. Разместите политики в корпоративной интрасети и рассмотрите необходимость ознакомления с ними всех новых сотрудников при приеме их на работу
Подкатегория	**Передовые методики**	
Управление учетными записями	Для всех пользователей, которым требуется доступ к ресурсам ИТ, необходимо создать отдельные учетные записи. Нельзя использовать общие учетные записи для нескольких пользователей. По умолчанию учетные записи должны создаваться с минимальными необходимыми привилегиями.	

Продолжение табл. 7.17

	Администраторы сетей и серверов должны иметь привилегированные (административные) и непривилегированные учетные записи. Стойкость пароля необходимо повышать и регулярно проверять, а все изменения учетной записи должны регистрироваться. По мере изменения роли отдельного пользователя все привилегии учетной записи должны быть пересмотрены и изменены при необходимости. В случае увольнения все учетные записи должны быть отключены или удалены	
Подкатегория	**Полученные данные**	**Рекомендации**
Управление учетными записями	Ваш ответ указывает на то, что в среде используются политики для главного управления учетными записями отдельных пользователей	Очень важно осуществлять управление учетными записями отдельных пользователей, используя политики, перечисленные в разделе, посвященном передовым методикам. Для среды на базе операционной системы Windows рассмотрите необходимость применения управления учетными записями пользователей с помощью Active Directory и периодически проверяйте стойкость паролей этих учетных записей. Для этих целей можно использовать самое разнообразное условно-бесплатное и бесплатное программное обеспечение, а также сторонние средства. Разработайте процедуры аудита и предупреждения для MOM (Microsoft Operations Manager) с целью отслеживания изменений прав учетной записи на серверах
	Вы указали, что стойкость пароля не применяется принудительно	Минимальная стойкость пароля должна быть определена политикой и затем усилена механизмом проверки подлинности

Окончание табл. 7.17

Подкатегория	**Передовые методики**	
Управление	Необходимо регулярно выполнять сторонние проверки, чтобы гарантировать соответствие всем требованиям законодательства	
Подкатегория	**Полученные данные**	**Рекомендации**
Управление	Вы указали, что в вашей организации существуют политики для управления вычислительной средой	Продолжите разработку и внедрение политик управления компьютерной средой в соответствии с действующими стандартами (ISO 17799, CoBIT, HIPAA, SOX и т. д.)
Подкатегория	**Передовые методики**	
Политика безопасности	Политики безопасности должны разрабатываться с участием руководителей, ИТ-специалистов и сотрудников отдела кадров, а также высшего руководства корпорации. Эти политики должны часто обновляться с учетом текущих передовых методик (например, CoBIT)	
Подкатегория	**Полученные данные**	**Рекомендации**
Политика безопасности	Вы указали, что у вас существует политика безопасности информации, направленная на регулирование деятельности организации, связанной с безопасностью	Продолжите использование политики информационной безопасности, однако периодически пересматривайте и обновляйте ее в соответствии с последними технологическими изменениями и изменениями среды
	Вы указали, что политика была разработана исключительно отделом ИТ	Политики должны разрабатываться как ИТ-специалистами, так и специалистами других отделов, чтобы учитывать юридические, технические и бизнес-требования

Таблица 7.18

Управление средствами исправления и обновления

Подкатегория	**Передовые методики**
Документация о сети	Всегда должны использоваться оперативные и точные физические и логические схемы внешних и внутренних сетей. Любые изменения, выполненные в этой среде, должны своевременно отражаться на соответствующей схеме. К схемам сетей должны иметь доступ только члены рабочей группы ИТ-специалистов

Продолжение табл. 7.18

Подкатегория	**Полученные данные**	**Рекомендации**
Документация о сети	Ваш ответ указывает на то, что в вашей среде отсутствуют логические сетевые схемы	Проведите работу с группой проектирования сети, чтобы сначала разработать схемы внешних сетей. Затем проведите работу по разработке схем для внутренней сети. Доступ к этим схемам должен иметь только ограниченный круг ИТ-специалистов и специалистов по безопасности
Подкатегория	**Передовые методики**	
Поток данных приложений	Схемы архитектуры приложений должны отображать основные компоненты и потоки важных данных в конкретной среде, включая системы, через которые проходят данные, а также способы их обработки. По мере выполнения обновления приложения или системы, содержащей это приложение, необходимо своевременно обновлять схемы	
Подкатегория	**Полученные данные**	**Рекомендации**
Поток данных приложений	Ваш ответ указывает на то, что для основных приложений не существует схем архитектуры приложений и потоков данных	Проведите работу с владельцами бизнеса, чтобы в первую очередь расположить в порядке приоритета внешние приложения, а затем внутренние. Располагая приложения в порядке приоритета, уделите внимание важности и критичности данных, которые обрабатываются с их помощью. Исходя из назначенного приоритета, проведите работу с группой архитектуры приложений и соответствующими владельцами бизнеса, чтобы составить окончательные схемы архитектуры и потоков данных для внешних приложений, а затем для любых внутренних приложений. Рассмотрите необходимость учреждения политики обновления этих схем в случае изменения среды

Окончание табл. 7.18

Подкатегория	**Передовые методики**	
Управление средствами исправления	Необходимо своевременно разворачивать изменения системы безопасности и конфигурации (в соответствии с корпоративной политикой безопасности) по мере их выхода. Исправления и обновления (разработанные собственными силами или предоставленные сторонними поставщиками) должны тщательно проверяться в лабораторных условиях до развертывания. Кроме того, необходимо проверить все системы после установки исправления, чтобы определить наличие конфликтов в конкретной системе, из-за которых может потребоваться выполнить откат исправления. Необходимо распределить системы по категориям, чтобы можно было осуществлять планирование на основе распределения по группам. Важные системы и системы с повышенным трафиком должны исправляться в первую очередь	
Подкатегория	**Полученные данные**	**Рекомендации**
Управление средствами исправления	Вы указали, что исправления и обновления проверяются перед их применением во всех системах	Продолжайте практику проверки всех исправлений и обновлений перед их развертыванием в рабочей среде
	Ваш ответ указывает на то, что политика исправлений и обновлений существует как для приложений, так и для операционных систем	Продолжайте осуществлять текущие процедуры и пересмотрите сведения, доступные в разделе, посвященном передовым методикам, чтобы внести все необходимые изменения в используемые политики. Оцените возможность использования серверов SMS и служб WSUS для автоматического администрирования
Подкатегория	**Передовые методики**	
Управление изменениями и конфигурация	Любые изменения в рабочей среде должны проверяться с точки зрения безопасности и совместимости перед запуском в производство, кроме того, должна вестись полная документация по конфигурации	
Подкатегория	**Полученные данные**	**Рекомендации**
Управление изменениями и конфигурация	Вы указали, что в вашей организации отсутствует процесс управления изменениями и конфигурацией	Рассмотрите необходимость реализации процесса официального управления изменениями и конфигурацией для проверки и документирования всех обновлений перед развертыванием

Таблица 7.19

Управление средствами исправления и обновления – ресурсы

Программная среда	Характеристика	Адрес в Интернете
Microsoft Update	Microsoft предоставляет автоматический способ регулярного получения последних обновлений продуктов и исправлений безопасности через службу Microsoft Update	http://www.update.microsoft.com/microsoftupdate/v6/vistadefault.aspx?ln=en-us
Microsoft Windows Server Update Services	Службы Microsoft Windows Server Update Services (WSUS) позволяют администраторам информационных технологий развертывать последние обновления продуктов Microsoft на компьютерах под управлением операционной системы Windows. Используя WSUS, администраторы могут полностью управлять распространением обновлений, выпущенных через Центр обновления Майкрософт, на компьютеры в своей сети	http://technet.microsoft.com/en-us/wsus/default.aspx
Systems Center Configuration Manager	System Center Configuration Manager 2007 – это решение для всесторонней оценки, развертывания и обновления серверов, клиентов и устройств в физических, виртуальных, распределенных и мобильных средах. Оптимизированное для Windows и расширяемое за ее пределами, оно представляет собой лучший выбор для получения более глубокого понимания и контроля над ИТ-системами	http://www.microsoft.com/system-center/configuration-manager/en/us/default.aspx

Таблица 7.20

Архивация и восстановление

Подкатегория	**Передовые методики**
Файлы журнала	Файлы журналов настроены на запись всех запланированных действий без перезаписи элементов. Необходимо настроить автоматическую процедуру чередования файлов журналов на ежедневной основе и разгрузить журналы на защищенный сервер в сети управления. Необходимо ограничить доступ к файлам журнала и настройкам конфигурации для предотвращения их изменения и удаления.

Продолжение табл. 7.20

Файлы журнала	Необходимо регулярно проверять файлы журналов на предмет подозрительной или аномальной активности. Проверка должна включать в себя контроль работы ИС, контроль обслуживания и контроль системы безопасности. Для расширения возможностей проверки необходимо использовать программное обеспечение корреляции событий и анализ тенденций	
Подкатегория	**Полученные данные**	**Рекомендации**
Файлы журнала	Ваш ответ показал, что в настоящее время в среде не ведутся файлы журналов	Включите сначала регистрацию на серверах и устройствах в DMZ, а также на основных серверах в сети. Определите идентичные конфигурации входа на аналогичных системах и обеспечьте защиту доступа к файлам журнала для предотвращения их изменения и удаления. Рассмотрите необходимость использования Microsoft Operations Manager (MOM) для отправки сигналов при создании критических записей в файлах журнала
Подкатегория	**Передовые методики**	
Планирование аварийного восстановления и возобновления деятельности предприятия	Продолжайте поддерживать и тестировать планы аварийного восстановления и возобновления деятельности предприятия. Требуйте разработки, документирования, реализации, а также периодических проверки, тестирования и обновления планов аварийного восстановления. Разработайте планы непрерывной работы предприятия, предусматривающие действия персонала, места размещений, а также системные и другие технологические проблемы. Проверьте открытые компоненты вместе с ИТ-специалистами своей компании или деловым партнером по обеспечению безопасности. Чтобы получить более подробные сведения, введите наиболее подходящий ответ на вопрос в средстве MSAT (Microsoft Security Assessment Tool).	

Продолжение табл. 7.20

	Планы аварийного восстановления и возобновления деятельности предприятия должны быть документально оформлены и соответствовать современным требованиям. Это позволит обеспечивать восстановление в приемлемые сроки. Планы (включая планы восстановления приложений из резервных копий) должны регулярно тестироваться на полноту и правильность. Планы непрерывной работы должны охватывать всю среду предприятия, включая ее физические и технологические составляющие, а также персонал	
Подкатегория	**Полученные данные**	**Рекомендации**
Планирование аварийного восстановления и возобновления деятельности предприятия	Ответ указывает на то, что организация выполняет процедуры аварийного восстановления и возобновления деятельности предприятия	Продолжайте поддерживать и тестировать планы аварийного восстановления и возобновления деятельности предприятия
	Ответ указывает на то, что организация не применяет процедуры аварийного восстановления и возобновления деятельности предприятия	Требуйте разработки, документирования, реализации, а также периодических проверки, тестирования и обновления планов аварийного восстановления. Разработайте планы непрерывной работы предприятия, предусматривающие действия персонала, места размещений, а также системные и другие технологические проблемы
	Вы указали, что не знаете ответа на этот вопрос	Проверьте открытые компоненты вместе с ИТ-специалистами своей компании или деловым партнером по обеспечению безопасности. Чтобы получить более подробные сведения, введите наиболее подходящий ответ на вопрос в средстве MSAT (Microsoft Security Assessment Tool)
Подкатегория	**Передовые методики**	
Архивация	Регулярно следует выполнять полную архивацию. Если возможно, необходимо выполнять частичную промежуточную архивацию между полными архивациями. В стратегии архивации должны рассматриваться наихудшие сценарии полного восстановления системы и приложения. Для важных приложений процесс восстановления должен полностью восстановить функции приложения за минимальное время	

Продолжение табл. 7.20

Подкатегория	**Полученные данные**	**Рекомендации**
Архивация	Ваш ответ указывает на то, что важные материалы в вашей среде архивируются на регулярной основе	Проведите аудит механизмов архивации и обеспечьте регулярное архивирование всех важных активов. Периодически проверяйте работоспособность функций восстановления, чтобы контролировать возможность восстановления с резервных носителей
Подкатегория	**Передовые методики**	
Резервные носители	Для управления хранением и работой резервных носителей должны применяться подробные политики. Эти политики должны касаться следующих аспектов: * хранения на месте/за пределами сети * чередования носителей * элементов управления безопасностью * элементов управления доступом персонала Съемные резервные носители необходимо хранить в запертых несгораемых корпусах, доступ к которым имеет только уполномоченный персонал. Необходимо хранить данные за пределами сети для повышения возможности их восстановления после сбоя	
Подкатегория	**Полученные данные**	**Рекомендации**
Резервные носители	Ваш ответ указывает на то, что в вашей среде все же существует политика, касающаяся хранения резервных носителей и работы с ними	Политика хранения резервных носителей и работа с ними – полезный начальный шаг, однако очень важно, чтобы эта политика была тщательно проработана и четко определена. Регулярно проводите аудит этой политики, чтобы обеспечить ее соответствие всем критериям
	Вы указали, что резервные копии не помещаются на хранение за пределами сети	Резервные носители необходимо хранить в запертых несгораемых корпусах за пределами сети, доступ к которым имеет только уполномоченный персонал. Их чередование и замена должны выполняться в соответствии с рекомендациями производителя

Окончание табл. 7.20

Подкатегория	**Передовые методики**	
Архивация и восстановление	Необходимо выполнять регулярные проверки процедур архивации и восстановления, чтобы определить сбойные носители и повысить вероятность успешного восстановления в случае сбоя. Необходимо подробно задокументировать все процедуры восстановления различных систем, включая приложения. Следует проверить все документы, посвященные архивации и восстановлению, чтобы убедиться, что в них описаны все критические системы, необходимые для непрерывного ведения бизнеса	
Подкатегория	**Полученные данные**	**Рекомендации**
Архивация и восстановление	Ваш ответ показал, что для процедур архивации и восстановления существует хорошо документированная политика	Следует проверить все документы, посвященные архивации и восстановлению, чтобы убедиться, что в них описаны все критические системы, необходимые для непрерывного ведения бизнеса. Регулярно проверяйте процедуры архивации и восстановления, чтобы контролировать надлежащее функционирование всех аппаратных и программных компонентов

Персонал. Усилия, направленные на обеспечение безопасности, часто не охватывают организационные аспекты, которые важны для поддержания общей безопасности в организации. В этом разделе оценки рассматриваются внутренние процессы предприятия, определяющие корпоративную политику безопасности, процессы, связанные с персоналом, осведомленность сотрудников о безопасности и их обучение. В области анализа, связанной с персоналом, также рассматривается безопасность применительно к повседневным операциям, относящимся к назначениям и определению ролей. Оценка предусматривает проверку процедур высокого уровня, которые организация может выполнять для снижения угрозы со стороны персонала, сосредоточившись на следующих областях безопасности, связанных с персоналом:

– требования и оценки: планирование, сторонние оценки;

– политика и процедуры: кадровая политика, сторонние взаимосвязи;

– обучение и осведомленность: осведомленность о безопасности (табл. 7.21 – 7.24).

Таблица 7.21

Персонал: требования и оценки

Подкатегория	**Передовые методики**	
Требования безопасности	Организации следует определить круг лиц, обладающих достаточной квалификацией по системам безопасности, которые должны участвовать во всех обсуждениях и принятии решений, связанных с безопасностью. Организация должна определить необходимые составляющие защиты на основе ценности имущества, а также уровень безопасности, требуемый для его защиты. Все векторы угроз включаются в анализ. Выработанная стратегия должна быть уравновешена с точки зрения расходов и преимуществ защиты. Кроме того, она может включать в себя передачу или принятие рисков. Требования по безопасности, полученные от представителей бизнеса и технических специалистов, должны быть задокументированы и опубликованы с целью ознакомления и будущего использования всеми сторонами. Различия между классами приложений и данных может привести к определению других конечных требований	
Подкатегория	**Полученные данные**	**Рекомендации**
Требования безопасности	Вы указали, что в вашей организации имеется модель для назначения уровней критичности каждому компоненту вычислительной среды	Продолжите назначение уровней важности для компонентов и обязательно обновляйте модель при добавлении нового оборудования
	Ваш ответ указывает на то, что в определение требований по безопасности вовлечены группы по безопасности и бизнесу	Группа, отвечающая за обеспечение безопасности, должна участвовать во всех мероприятиях, связанных с разработкой требований, проектированием и развертыванием технологий. Требования по безопасности должны быть четко задокументированы и являться частью функциональных требований

Окончание табл. 7.21

Подкатегория	**Передовые методики**	
Оценки безопасности	Необходимо провести стороннюю оценку, чтобы получить полезную и объективную точку зрения на состояние системы безопасности организации. Сторонние оценки могут быть также полезны для обеспечения соответствия требованиям нормативов, клиентов, партнеров и поставщиков. Оценки должны затрагивать инфраструктуру, приложения, политики, а также процедуры аудита. Целью этих оценок должно быть не только определение проблем безопасности, но также проверка небезопасных конфигураций и прав внешнего доступа. Необходимо проверить и оценить политики и процедуры безопасности на предмет пробелов	
Подкатегория	**Полученные данные**	**Рекомендации**
Оценки безопасности	Вы указали, что оценки безопасности для вашей организации выполняются внутренним персоналом	Продолжайте практику частых проверок безопасности внутренним персоналом, но в дополнение к этому привлекайте заслуживающую доверия стороннюю организацию
	Вы указали, что независимые оценки безопасности не выполнялись третьими сторонами	Начните с самостоятельной оценки важных элементов инфраструктуры сети и приложений. Рассмотрите необходимость составления плана, предусматривающего проведение регулярной плановой независимой оценки важных элементов инфраструктуры сети и приложений. Используйте результаты этих оценок в проектах, направленных на совершенствование

Таблица 7.22

Персонал: политика и процедуры

Подкатегория	**Передовые методики**	
Проверка в фоновом режиме	Для определения любых потенциальных проблем необходимо проводить проверки в фоновом режиме, тем самым снижая риск для организации и других служащих. Этот шаг также позволяет определить любые потенциальные проблемы и пробелы в резюме кандидата. Процесс найма должен включать в себя обзор предыдущих мест работы кандидата и сведения о привлечении к юридической ответственности. Необходимо оценить навыки кандидата с точки зрения подробных должностных инструкций и требований, чтобы понять его сильные и слабые стороны	
Подкатегория	**Полученные данные**	**Рекомендации**
Проверка в фоновом режиме	Ваш ответ указывает на то, что в вашей организации в данный момент не проводится проверка в фоновом режиме в качестве обычной составляющей процесса найма	Реализуйте политику, требующую проверки биографических данных и репутации для всех новых лиц, которые будут занимать важные должности. Со временем эта политика должна начать действовать в отношении всех вновь нанимаемых сотрудников независимо от занимаемой ими должности
Подкатегория	**Передовые методики**	
Политика отдела кадров	Формальная процедура увольнения должна гарантировать, что предприняты все необходимые шаги при завершении трудового соглашения. Должны существовать процедуры для увольнения как по обычным причинам, так и в результате конфликтов. Эти процедуры должны включать в себя следующее: * уведомление всех отделов: отдела кадров, ИТ, физической защиты, службы поддержки, финансового отдела и т. д. * выдворение служащего за пределы компании * удаление всех учетных записей и прекращение доступа к сети * сдача собственности, принадлежащей компании: переносных и карманных компьютеров, электронных носителей, конфиденциальных документов и т. д.	

Продолжение табл. 7.22

Подкатегория	**Полученные данные**	**Рекомендации**
Политика отдела кадров	Ваш ответ указывает на то, что в вашей организации существует официальная недружелюбная политика в отношении служащих, покидающих компанию	Регулярно проверяйте существующие процедуры увольнения недружелюбно настроенных сотрудников и вносите обновления, связанные с упущениями, на основе опыта прошлых увольнений
	Ваш ответ указывает на то, что в вашей организации существует дружественная политика в отношении служащих, покидающих компанию	Периодически проверяйте существующую дружественную политику в отношении увольняющихся сотрудников и рассматривайте любые выявленные недостатки
Подкатегория	**Передовые методики**	
Сторонние взаимосвязи	Чтобы снизить риск разглашения данных, необходимо применять формальные политики и процедуры для урегулирования взаимоотношений со сторонними компаниями. Эти политики и процедуры позволяют определить проблемы безопасности и ответственность каждой из сторон при их устранении. Эти политики должны включать в себя следующее: * уровень соединения и доступа * представление данных и работу с ними * роли и ответственность (включая полномочия) каждой стороны * управление взаимоотношениями: установление, продолжение и прекращение	
Подкатегория	**Полученные данные**	**Рекомендации**
Сторонние взаимосвязи	Вы указали, что конфигурирование систем выполняется персоналом	Системы должны настраиваться внутренним персоналом в соответствии с проверенным образом
	Вы указали, что ваша организация самостоятельно осуществляет управление вычислительной средой	В зависимости от потребностей бизнеса, подходящим решением будет самоуправление или привлечение внешних ресурсов. Если управление осуществляется с использованием внешних ресурсов, требования по безопасности необходимо оговорить в контракте, а соглашения об уровне сервиса (SLA) предназначены для обеспечения соответствия этим требованиям

Окончание табл. 7.22

Сторонние взаимосвязи	Ваш ответ указывает на отсутствие политики регулирования сторонних взаимосвязей	Формальные политики и процедуры для всех типов сторонних взаимосвязей должны быть разработаны и согласованы во всех отделах организации. При формировании этих политик включайте в них разнообразные бизнес-группы, отвечающие за эти взаимосвязи

Таблица 7.23

Персонал: обучение и осведомленность

Подкатегория	**Передовые методики**	
Осведомленность о безопасности	Программа уведомления о вопросах безопасности позволяет служащим внести свой вклад в общее состояние системы безопасности компании благодаря информированию их о последних угрозах безопасности. Хорошо осведомленные служащие могут немедленно сообщить о проблемах безопасности. В эффективной программе осведомленности должны учитываться все аспекты безопасности, включая приложение, сеть и физические устройства, а также содержаться четкие инструкции относительно обязанностей служащих в случае обнаружения ими того, что может подвергнуть опасности любой из этих элементов. Следует реализовать политики, которые регулируют использование служащими ресурсов компании. Программа осведомленности должна стать составной частью обучения нового персонала. Необходимо регулярно проводить курсы повышения квалификации и переподготовки, чтобы гарантировать, что все служащие знакомы с последними практиками и рисками. Чтобы гарантировать полное понимание служащими этого материала, необходимо проводить регулярные проверки	
Подкатегория	**Полученные данные**	**Рекомендации**
Осведомленность о безопасности	Вы указали, что в вашей организации в отношении безопасности существует индивидуальная или групповая ответственность	Продолжайте поддерживать в компании специалиста или группу специалистов, ответственных за безопасность, и требуйте обязательной консультации с этими сотрудниками перед изменением вычислительной среды

Продолжение табл. 7.23

	Вы указали, что группа, обеспечивающая безопасность в вашей организации, участвует в определении требований для новых и существующих технологий	Продолжайте практику консультации со специалистом/группой специалистов по безопасности перед изменением вычислительной среды. Консультироваться с группой специалистов по безопасности необходимо на ранних стадиях планирования
	Ваш ответ указывает на то, что в вашей организации все же существует программа осведомленности о вопросах безопасности	Все сотрудники должны участвовать в обучении по вопросам осведомленности. Осведомленность о вопросах безопасности должна стать обязательной составной частью обучения нового персонала. Хорошо осведомленные служащие могут немедленно сообщить о проблемах безопасности
	Вы указали, что обучение проводится ежегодно	Обучение по вопросам безопасности должно проводиться для всех сотрудников ежеквартально
	Вы указали, что в программе уведомления о вопросах безопасности участвовало более 75 % всех служащих	Продолжайте практику обязательного участия всех сотрудников в обучении по вопросам осведомленности о безопасности. Осведомленность о вопросах безопасности должна стать обязательной составной частью обучения нового персонала. Хорошо осведомленные служащие могут немедленно сообщить о проблемах безопасности
	Вы указали, что обучение, связанное с осведомленностью, не охватывает безопасность средств Интернета, включая веб-просмотр и загрузку файлов с узлов	Обучение по вопросам безопасности должно затрагивать все аспекты, включая средства контроля и политики безопасности, сообщение о подозрительных действиях, конфиденциальность, безопасность электронной почты, безопасность Интернета и компьютера

Окончание табл. 7.23

	Вы указали, что обучение, связанное с осведомленностью, не охватывает безопасность компьютера, включая использование персональных межсетевых экранов и шифрование	Обучение по вопросам безопасности должно затрагивать все аспекты, включая средства контроля и политики безопасности, сообщение о подозрительных действиях, конфиденциальность, безопасность электронной почты, безопасность Интернета и компьютера
Подкатегория	**Передовые методики**	
Обучение в области безопасности	В сотрудничестве с владельцами предприятий определите приемлемую продолжительность простоя для критически важных приложений. Основываясь на полученных данных, примите необходимые меры, чтобы обеспечить полное соответствие выработанным требованиям. Доступность и производительность веб-приложений можно улучшить за счет развертывания подсистем балансировки нагрузки перед веб-серверами. Принцип работы подсистемы балансировки нагрузки заключается в распределении запросов на разные узлы в кластере серверов с целью оптимизации производительности системы. Если на одном веб-сервере в кластере серверов происходит сбой, запрос перенаправляется для обработки на другой сервер, что обеспечивает высокий уровень доступности. В сотрудничестве с владельцами предприятий определите приемлемую продолжительность простоя для критически важных файловых ресурсов и баз данных. Протестируйте механизмы перехода приложений на другие ресурсы при сбое и определите соответствие продолжительности простоя приемлемым значениям	
Подкатегория	**Полученные данные**	**Рекомендации**
Обучение в области безопасности	Ваш ответ указывает на то, что в вашей организации в данный момент не проводится тематическое обучение для служащих	Разработайте сначала план для группы ИТ, а при необходимости и для инженеров-разработчиков в соответствии со своей бизнес-моделью для посещения соответствующих курсов обучения по безопасности. Начните реализацию плана с посещения участниками группы внешнего обучения в виде семинаров и тематического обучения по вопросам безопасности

Таблица 7.24

Персонал: обучение и осведомленность – ресурсы

Программная среда	Характеристика	Адрес в Интернете
Microsoft Security Certifications	Сертификация MCSE: Security for Windows Server 2003 дает вам набор навыков для защиты среды Windows Server	http://www.microsoft.com/learning/mcp/mcse/security/windowsserver2003.mspx
Industry Security Certifications	ISC2 – сертификаты CISSP, SSCP ISACA – сертификаты CISM, CISA CompTIA – Security+	http://www.isc2.org http://www.isaca.org http://www.comptia.org
Microsoft Security Awareness Toolkit	Корпорация Майкрософт признает, что осведомленность и обучение информационной безопасности имеют решающее значение для стратегии информационной безопасности любой организации и поддержки операций по обеспечению безопасности. Во многих случаях люди являются последней линией защиты от таких угроз, как вредоносный код, недовольные сотрудники и злонамеренные третьи лица. Таким образом, люди должны быть осведомлены о том, что́ ваша организация считает надлежащим поведением с точки зрения безопасности, а также о том, какие передовые методы обеспечения безопасности им необходимо использовать в своей повседневной деловой деятельности. Этот комплект был создан, чтобы предоставить руководство, примеры и шаблоны для создания вашей собственной программы обеспечения безопасности	http://technet.microsoft.com/en-us/security/cc165442. aspx

Список приоритетных действий представлен в табл. 7.25.

Таблица 7.25

Список приоритетных действий

Предмет анализа	Рекомендация
Высокий приоритет	
Инфраструктура > Управление и контроль > Защищенная сборка	Продолжайте практику обязательной установки на компьютеры всех пользователей экранной заставки с парольной защитой с коротким периодом ожидания
Инфраструктура > Защита по периметру > Сегментация	Убедитесь в наличии межсетевого экрана, сегментирования и систем определения вторжения для защиты инфраструктуры компании от атак из Интернета
Персонал > Политика и процедуры > Сторонние взаимосвязи	Системы должны настраиваться внутренним персоналом в соответствии с проверенным образом
Приложения > Развертывание и использование > Независимый сторонний поставщик программного обеспечения	Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на этот вопрос в средстве MSAT для получения дальнейших сведений
Операции > Архивация и восстановление > Планирование аварийного восстановления и возобновления деятельности предприятия	Продолжайте поддерживать и тестировать планы аварийного восстановления и возобновления деятельности предприятия
Средний приоритет	
Персонал > Требования и оценки > Оценки безопасности	Начните с самостоятельной оценки важных элементов инфраструктуры сети и приложений. Рассмотрите необходимость составления плана, предусматривающего проведение регулярной плановой независимой оценки важных элементов инфраструктуры сети и приложений. Используйте результаты этих оценок в проектах, направленных на совершенствование
Инфраструктура > Защита по периметру > Система определения вторжения (IDS)	Продолжайте практику развертывания сетевой системы определения вторжения. Следите за регулярным обновлением сигнатур вирусов, а также изучайте технологии предотвращения вторжения
Операции > Политика безопасности > Классификация данных	Продолжайте реализовывать классификацию данных с соответствующими рекомендациями по защите

Окончание табл. 7.25

Операции > Политика безопасности > Утилизация данных	Продолжайте реализовывать процедуры удаления данных
Приложения > Развертывание и использование > Внутренняя разработка	Постарайтесь по-прежнему не использовать собственные макросы Office, поскольку использование собственных макросов означает, что настройки безопасности пакета Office необходимо понизить, в результате чего офисные приложения могут быть подвержены заражению документами злоумышленников
Низкий приоритет	
Операции > Среда > Узел управления – Серверы	Рассмотрите необходимость использования SSH или VPN для защиты текстовых протоколов
Операции > Среда > Узел управления – Сетевые устройства	Следует протестировать все системы управления, в которых используется SNMP, чтобы убедиться, что в них используются последние версии исправлений и не используются настройки сообщества по умолчанию
Операции > Политика безопасности > Правильное использование	Все сотрудники и клиенты, использующие корпоративные ресурсы, должны быть ознакомлены с этими политиками. Разместите политики в корпоративной интрасети и рассмотрите необходимость ознакомления с ними всех новых сотрудников при приеме их на работу
Операции > Архивация и восстановление > Архивация	Проведите аудит механизмов архивации и обеспечьте регулярное архивирование всех важных активов. Периодически проверяйте работоспособность функций восстановления, чтобы контролировать возможность восстановления с резервных носителей
Инфраструктура > Защита по периметру > Антивирус – Настольные компьютеры	Продолжайте использовать такую практику. Реализуйте политику, в соответствии с которой пользователям необходимо регулярно обновлять сигнатуры вирусов. Рассмотрите необходимость установки клиента антивирусной программы с использованием настроек для рабочей станции по умолчанию

ВАРИАНТЫ ИСХОДНЫХ ЗАДАНИЙ ДЛЯ КУРСОВОЙ РАБОТЫ

Все планировки объектов выдаются обучающимся в электронном виде, в том числе:

– поэтажные планы объекта;

– генплан расположения объекта на местности;

– поэтажные планы расположения по помещениям средств вычислительной техники.

Вариант № 1

Объект – строительная коммерческая организация ООО (название придумать самостоятельно), занимающая часть 1-го этажа пятиэтажного кирпичного здания с подвалом и круглосуточным постом охраны. В здании подвал, смежные помещения и другие этажи занимают (арендуют) прочие «не охраняемые» собственники.

Перекрытия полов и потолков капитальные, из железобетонных панелей. Все внутренние двери деревянные, филенчатые, полнотелые. Двери в служебные кабинеты и бухгалтерию, кассу, архив, сейфовую комнату, серверную, пост охраны и другие имеют по одному врезному замку. Двери в холлах, коридорах, тамбурах и на лестничных клетках остекленные в верхней половине двери и запорных устройств не имеют. Все внутренние перегородки и стены (кроме наружных по периметру здания) гипсокартонные, каркасные или в кирпич (полкирпича), некапитальные. Во всех служебных кабинетах имеются персональные компьютеры, на складах – дорогостоящие материальные ценности. В помещениях 9, 16, 38 установлены сейфы массой 150 – 200 кг без крепления к полу и стенам. Кабинет 21 – защищаемое режимное помещение с отработкой информации, составляющей коммерческую тайну.

Двери:

Д1 – дверь цельнометаллическая, с одним врезным замком

Д2 – дверь пластиковая, с одним врезным замком, верхняя половина двери остеклена

Д3 – дверь деревянная, полнотелая, филенчатая, с одним врезным замком

Д4 – ворота деревянные, цельные, с одним наружным навесным замком

Д5 – дверь цельнометаллическая, с двумя врезными замками на расстоянии более 300 мм

Решетчатые раздвижные двери за входными дверями в здание отсутствуют.

Окна:

О1 – окно с деревянными рамами и двойным остеклением, без защитных пленок, решетки отсутствуют

О2 – окно пластиковое, с двойным остеклением, без защитных пленок, решетки отсутствуют

О3 – окно деревянное, с двойным остеклением, без защитных пленок, решетка со стороны улицы из прутка D = 12 мм, размер ячейки 200×200 мм

Экспликация помещений объекта:

1 – холл; 2, 3 – архив; 4 – комната хозинвентаря; 5 – 6 – служебные кабинеты; 7 – 8 – коридор; 9 – касса; 10 – главный бухгалтер; 11 – бухгалтерия; 12 – лестничная клетка; 13 – 16 – служебные кабинеты; 17 – коридор; 18 – фойе; 19 – 20 – служебные кабинеты; 21 – канцелярия; 22 – фойе; 23 – пост охраны; 24 – 26 – служебные кабинеты; 27 – 29 – служебные кабинеты; 30 – кабинет начальника; 31 – приемная; 32 – коридор; 33 – 36 – служебные кабинеты; 37 – серверная; 38 – 39 – служебные кабинеты; 40 – фойе; 41 – тамбур; 42 – подсобное помещение; 43 – склад; 44 –лестничная клетка

Структура организации

Во главе ООО стоит генеральный директор (каб. 30), у которого три заместителя.

Непосредственно руководителю подчиняется:

– канцелярия (каб. 38), в штате: зав. канцелярией и два секретаря (один – в каб. 38 и один – в приемной (пом. 31)), зав. архивом (пом. 2);

– служба безопасности (пом. 23 – 26), в штате: начальник СБ (каб. 25) и подразделения (группа охраны и режима – ст. инспектор и два инспектора (каб. 24); группа режима КИ – один инспектор (каб. 38); группа ИБ и ТЗИ – один администратор безопасности (каб. 21), ст. инспектор и инспектор (каб. 26), ст. юрисконсульт по безопасности, юрисконсульт по безопасности (каб. 35)).

1-й заместитель – по экономике (каб. 31 – приемная). Ему подчиняются:

– бухгалтерия с кассой (каб. 9 – 11), в штате: гл. бухгалтер (каб. 10), экономист, два бухгалтера (каб. 11), кассир (каб. 9);

– планово-экономический отдел (каб. 5 – 6), в штате: начальник отдела (каб. 6), ст. экономист, экономист, инженер 2-й категории;

– отдел маркетинга (каб. 27 – 28), в штате: начальник отдела (каб. 28), ст. маркетолог-аналитик, два маркетолога-аналитика, бренд-менеджер; менеджер по торговым маркам и продуктам (все занимают каб. 27).

2-й заместитель – главный инженер (каб. 39). Ему подчиняются:

– отдел капитального строительства (каб. 13 – 16), в штате: начальник отдела (каб. 16), гл. специалист, ст. специалист, два инженера 1-й категории (каб. 15), инженер по техническому надзору (каб. 14), три инженера 1-й категории (каб. 13);

– проектно-сметная группа (каб. 39), в штате: ст. инженер-проектировщик и инженер-сметчик;

– служба автоматизации (IT) (каб. 21), в штате: системный администратор и инженер технической поддержки 1-й категории.

3-й заместитель – по общим вопросам (каб. 31 – приемная). Ему подчиняются:

– оперативно-диспетчерская служба (каб. 19 – 20), в штате: три ст. диспетчера, зав. гаражом (каб. 42), пять водителей, кладовщик (каб. 43);

– группа по охране труда и технике безопасности (ОТ и ТБ) (каб. 29), в штате: ст. инженер по ОТ и ТБ, инженер по ТБ и пожарной безопасности;

– отдел кадров и оргштатной работы (каб. 33 – 34), в штате: начальник отдела (каб. 33), ст. инспектор отдела кадров, инспектор отдела кадров, инспектор оргштатной работы.

В подчинении начальнику отдела кадров находятся: слесарь-сантехник – 0,5 ставки, электрик – 0,5 ставки, дворник – 0,5 ставки, уборщицы – 1,5 ставки.

В структуре СБ основные задачи структурных подразделений следующие:

– группа охраны и режима: контроль обеспечения охраны объекта со стороны частной охранной организации, контроль работоспособности ОТС, СКУД и СВН, контроль эксплуатационно-технического

обслуживания данных систем, обеспечение КПиОР, доставка ценных грузов, проверка почтовых сообщений;

– группа режима КИ: контроль ведения конфиденциального делопроизводства, работа с персоналом и посетителями, контроль публикаторской и издательской деятельности, работа со СМИ, контроль обеспечения режима КТ;

– группа ИБ и ТЗИ: администрирование безопасности ЛВС и ЭВМ, защищенные технологии обработки информации, техническая защита от утечки информации по техническим каналам;

– юрисконсульт по безопасности: юридическое сопровождение обеспечения безопасности, организационное обеспечение ИБ, аналитическая работа.

Штатный персонал объекта: общая характеристика (кроме обслуживающего персонала, основных и вспомогательных рабочих)

№ п/п	Структурное подразделение	Расположение (номер кабинета/номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
1	Руководство	30/23	Гендиректор/8	23, 31, 24	Высшее техническое профильное	5	3
2	Руководство	31/25	Зам. по экономике/4	25, 24	Высшее экономическое	4	3
3	Руководство	39/31	Гл. инженер/5	31, 29	Высшее техническое профильное	7	4
4	Руководство	31/26	Зам. по общим вопросам/9	26, 24	Высшее техническое профильное	3	1
5	Канцелярия	38/27	Зав. канцелярией/2	27, 24, 54	Высшее техническое	7	6
6	Канцелярия	31/24	Секретарь/2	24, 23, 27, 54	Среднее специальное	2	1
7	Канцелярия	38/27	Секретарь/4	27, 24, 54	Высшее гуманитарное	3	2

Продолжение

№ п/п	Структурное подразделение	Расположение (номер кабинета/номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
8	Канцелярия	2/54	Зав. архивом/12	54, 27, 24	Высшее гуманитарное	3	2
9	Служба безопасности	25/41	Начальник СБ/3	41, 28, 43	Высшее военное	4	2
10	Служба безопасности	24/42	Ст. инспектор СБ/3	42, 43	Высшее техническое профильное	5	5
11	Служба безопасности	24/42	Инспектор СБ/2	42, 43	Высшее гуманитарное	6	5
12	Служба безопасности	24/42	Инспектор СБ/5	42	Высшее техническое профильное	6	5
13	Служба безопасности	38/28	Инспектор группы режима КИ/7	28, 24, 54	Высшее гуманитарное	5	5
14	Служба безопасности	21/44 (37/34)	Администратор безопасности/3	Все (1 – 54)	Высшее техническое профильное	9	9
15	Служба безопасности	26/39	Ст. инспектор СБ (ИБ и ТЗИ)/2	39, 40	Высшее техническое профильное	5	5
16	Служба безопасности	26/40	Инспектор СБ (ИБ и ТЗИ)/4	40, 39	Высшее военное	7	6
17	Служба безопасности	35/35	Ст. юрисконсульт/3	35	Высшее военное	5	5
18	Служба безопасности	35/35	Юрисконсульт/7	35	Высшее юридическое	6	6

Продолжение

№ п/п	Структурное подразделение	Расположение (номер кабинета/номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
19	Бухгалтерия	10/1	Гл. бухгалтер/9	1, 2, 3, 4, 5	Высшее экономическое	2	2
20	Бухгалтерия	11/3	Экономист/4	3, 4, 5, 2	Высшее экономическое	2	2
21	Бухгалтерия	11/4	Бухгалтер/5	4, 2, 3, 5	Высшее экономическое	3	3
22	Бухгалтерия	11/5	Бухгалтер/8	5, 2, 3, 4	Среднее специальное	2	2
23	Бухгалтерия	9/2	Кассир/2	2, 3	Среднее специальное	1	1
24	Планово-экономический отдел	6/51	Начальник планово-экономического отдела/6	51, 50, 52, 53	Высшее экономическое	5	5
25	Планово-экономический отдел	5/50	Ст. экономист/3	50, 52	Высшее экономическое	4	4
26	Планово-экономический отдел	5/52	Экономист/4	52, 50	Высшее экономическое	4	3
27	Планово-экономический отдел	5/53	Инженер 2-й категории/3	53, 50, 52	Высшее экономическое	3	3
28	Отдел маркетинга	28/20	Начальник отдела маркетинга/6	20, 15, 16, 17	Высшее экономическое	3	2
29	Отдел маркетинга	27/15	Ст. маркетолог-аналитик/4	15, 16	Среднее специальное	4	3
30	Отдел маркетинга	27/16	Маркетолог-аналитик/5	16, 15	Высшее экономическое	3	2

Продолжение

№ п/п	Структурное подразделение	Расположение (номер кабинета/номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
31	Отдел маркетинга	27/17	Маркетолог-аналитик/8	17, 18	Среднее специальное	4	2
32	Отдел маркетинга	27/18	Бренд-менеджер/3	18, 17	Среднее специальное	5	4
33	Отдел маркетинга	27/19	Менеджер по торговым маркам и продуктам/2	19, 18, 16, 17	Высшее экономическое	2	2
34	Отдел капитального строительства (ОКС)	16/14	Начальник отдела/5	14, 10, 11, 12, 13, 6, 7, 8, 9	Высшее техническое профильное	3	3
35	ОКС	15/10	Гл. специалист/3	10, 11, 12, 13, 6, 7	Высшее техническое	5	5
36	ОКС	15/11	Ст. специалист/7	11, 12, 13	Высшее техническое профильное	5	5
37	ОКС	15/12	Инженер 1-й категории/3	12, 13	Высшее техническое профильное	4	4
38	ОКС	15/13	Инженер 1-й категории/7	13, 12	Высшее техническое	3	3
39	ОКС	14/9	Инженер по технадзору/2	9, 6	Высшее техническое профильное	4	4
40	ОКС	13/6	Инженер 1-й категории/4	6, 9	Высшее техническое	5	4
41	ОКС	13/7	Инженер 1-й категории/6	7, 8	Высшее техническое профильное	4	3

Продолжение

№ п/п	Структурное подразделение	Расположение (номер кабинета/номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
42	ОКС	13/8	Инженер 1-й категории/3	8, 9	Высшее техническое профильное	3	2
43	Проектно-сметная группа	39/29	Ст. инженер-проектировщик/3	29, 30	Высшее техническое профильное	7	6
44	Проектно-сметная группа	39/30	Инженер-сметчик/2	30, 29	Высшее экономическое	3	1
45	Служба автоматизации (IT)	21/45 (37/34)	Системный администратор/4	Все (1 –54)	Высшее техническое	10	8
46	Служба автоматизации (IT)	21/46	Инженер технической поддержки 1-й категории/8	Все (1 – 54)	Высшее техническое профильное	9	8
47	Оперативно-диспетчерская служба (ОДС)	20/47	Ст. диспетчер/5	47, 48, 49, 33	Высшее экономическое	4	2
48	ОДС	20/48	Ст. диспетчер/4	47, 48, 49, 33	Высшее техническое	3	3
49	ОДС	20/49	Ст. диспетчер/7	47, 48, 49, 33	Высшее экономическое	4	3
50	ОДС	42/33	Зав. гаражом/8	47, 48, 49, 33	Высшее техническое	3	2
51	ОДС	43/32	Кладовщик	32	Среднее специальное	3	2
52	Группа по ОТ и ТБ	29/21	Ст. инженер по ОТ и ТБ/5	21, 22	Высшее техническое	4	2

Окончание

№ п/п	Структурное подразделение	Расположение (номер кабинета/номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
53	Группа по ОТ и ТБ	29/22	Инженер по ТБ и пожарной безопасности/4	21, 22	Высшее техническое	3	2
54	Отдел кадров и орг-штатной работы	33/38	Начальник отдела/2	38, 36, 37	Высшее техническое	3	2
55	Отдел кадров и орг-штатной работы	34/36	Ст. инспектор ОК/7	36, 37	Высшее техническое	4	3
56	Отдел кадров и орг-штатной работы	34/36	Инспектор ОК/3	36, 37	Высшее экономическое	2	2
57	Отдел кадров и орг-штатной работы	34/37	Инспектор орг-штатной работы/5	37, 36	Среднее специальное	3	1

Структура защищаемой информации

№ п\п	Наименование источника информации	Гриф	Источник информации	Место нахождения источника информации
1	Структура предприятия	К	Контракты, документы на бумажных носителях, персонал	Сейф с документами, каб. 38; ПК 27, 54
2	Личные сведения о сотрудниках фирмы	ПДн	Документы на бумажных и электронных носителях, БД, персонал фирмы	Сейф с документами, каб. 9; ПК 2, 1, 3, 36, 38

Продолжение

№ п\п	Наименование источника информации	Гриф	Источник информации	Место нахождения источника информации
3	Учредительные документы	К	Устав организации, бумажные документы	Рабочий стол в кабинете директора, секретаря; ПК 27, 54
4	Сведения о кредитах, контрактах	К	Документы на бумажных и электронных носителях, БД, гл. бухгалтер	Сейф с документами, каб. 9; ПК 2, 1, 4, 51
5	База данных заказчиков, партнеров фирмы	КТ	Документы на бумажных и электронных носителях, гл. бухгалтер	Сейф с документами, каб. 9; ПК 2, 4, 51
6	Сведения о конкурентах (в том числе компромат)	КТ	Документы на бумажных и электронных носителях	Сейф с документами, каб. 38; ПК 23, 24, 41
7	Сведения о распределении прибыли между сотрудниками	К	Документы на бумажных и электронных носителях, гл. бухгалтер	Сейф с документами, каб. 9; ПК 2, 1, 3, 36, 38
8	Список отсутствующих сотрудников, сроки их отсутствия	СК	Документы на бумажных и электронных носителях, бухгалтерия, ОК	Сейф с документами, каб. 9; ПК 2, 1, 3, 36, 38
9	Пароли к используемому ПО и web-сайтам	КТ	Документы на электронных носителях, СБ, отдел IT	ПК 34, 45, 46, 44
10	Архив различных версий разрабатываемых ПО, web-сайтов	СК	Документы на электронных носителях, СБ, отдел IT	ПК 34, 45, 46, 44, 54
11	Архив названий, логотипов, рекламных буклетов и роликов фирм-заказчиков	СК	Документы на бумажных и электронных носителях, отдел маркетинга	Сейф с документами, каб. 38; ПК 18, 19, 20
12	Сведения о концепте и продвижении продукции	КТ	Документы на бумажных и электронных носителях, отдел маркетинга	Сейф с документами, каб. 38; ПК 18, 19, 20

Окончание

№ п\п	Наименование источника информации	Гриф	Источник информации	Место нахождения источника информации
13	Методы и способы производства, новые технологии	КТ	Документы на бумажных и электронных носителях, отдел маркетинга	Сейф с документами, каб. 21; ПК 14
14	Конкурентоспособность производимой продукции, эффективность экспорта и импорта, предполагаемое время выхода на рынок	СК	Документы на бумажных и электронных носителях, отдел маркетинга	Сейф с документами, каб. 38; ПК 18, 19, 20
15	Планы и характер рекламной и публикаторской деятельности	КТ	Документы на бумажных и электронных носителях, юрисконсульты	Сейф с документами, каб. 38; ПК 35
16	Кадровый состав и его формирование	СК	Документы на бумажных и электронных носителях, бухгалтерия, ОК, стол директора	Сейф с документами, каб. 9; ПК 1, 36, 38
17	Сведения о системе безопасности организации	КТ	Документы на бумажных и электронных носителях, СБ, рабочий стол директора	Сейф с документами, каб. 38; ПК 41, 42, 43
18	Телефонные переговоры сотрудников и клиентов	КТ	Документы на электронных носителях, СБ, отдел IT	ПК 41, 42, 43
19	Направления модернизации известных технологий, процессов и оборудования	КТ	Документы на бумажных и электронных носителях, отдел маркетинга	Сейф с документами, каб. 21; ПК 14
20	Изобретения и полезные модели, используемые инновации и ноу-хау производства	КТ	Документы на бумажных и электронных носителях, отдел маркетинга	Сейф с документами, каб. 21; ПК 14

Вариант № 2

Объект – организация оптовой торговли (оргтехника, системы связи) ООО (название придумать самостоятельно), занимающая 1-й этаж трехэтажного кирпичного здания с подвалом и дневным постом охраны. В здании подвал и другие этажи занимают (арендуют) прочие «не охраняемые» собственники.

Перекрытия полов и потолков капитальные, из железобетонных панелей. Все внутренние двери деревянные, филенчатые, полнотелые. Двери в служебные кабинеты и бухгалтерию, кассу, архив, канцелярию, серверную, пост охраны и другие имеют по одному врезному замку. Двери в холлах, коридорах, тамбурах и на лестничных клетках остекленные в верхней половине двери и запорных устройств не имеют. Все внутренние перегородки и стены (кроме наружных по периметру здания) гипсокартонные, каркасные или в кирпич (полкирпича), не капитальные. Капитальной является горизонтальная кирпичная стена по центру здания. Во всех служебных кабинетах имеются персональные компьютеры, на складе – дорогостоящие материальные ценности. В помещениях 19, 9 и кассы установлены сейфы массой 150 – 200 кг без крепления к полу и стенам. Кабинет 9 – защищаемое режимное помещение с хранением информации, составляющей коммерческую тайну.

Двери:

Д1 – дверь цельнометаллическая, с двумя врезными замками на расстоянии менее 300 мм

Д2 – дверь цельнометаллическая, с двумя врезными замками на расстоянии более 300 мм

Д3 – дверь пластиковая, с двумя врезными замками на расстоянии менее 300 мм, верхняя половина двери остеклена

Д4 – дверь решетчатая, раздвижная, с одним врезным замком

Д5 – дверь пластиковая, полнотелая, с двумя врезными замками на расстоянии более 300 мм

Окна:

О1 – окно пластиковое, с двойным остеклением, без защитных пленок, без решеток

О2 – окно пластиковое, с двойным остеклением, без защитных пленок, решетка со стороны помещения из прутка D = 16 мм, размер ячейки 120×150 мм

О3 – окно пластиковое, с двойным остеклением, без защитных пленок, решетка со стороны помещения из прутка D = 16 мм, размер ячейки 120×150 мм

О4 – окно пластиковое, с двойным остеклением, без защитных пленок, решетка со стороны помещения из прутка D = 16 мм, размер ячейки 120×150 мм

В помещениях 3, 10, 11 решетки на окнах отсутствуют.

Экспликация помещений объекта:

1 – тамбур; 2 – коридор; 3 – офисное помещение; 4 – тамбур; 5 – пост охраны; 6 – диспетчерская; 7 – электрощитовая; 8, 30 – служебные кабинеты; 9 – канцелярия; 10 – коридор; 11 – бухгалтерия; 12 – санузел; 13 – юристы; 14 – тамбур; 15 – служебный кабинет; 16 – холл; 17 – лестничная клетка; 18 – тамбур; 19 – 20 – служебные кабинеты; 21 – склад; 22 – коридор; 23 – 24 – служебные кабинеты; 25 – тамбур; 26 – архив; 27, 28 – технические помещения; 29 – серверная; 31 – коридор; 32 – служебный кабинет; 33 – приемная.

Структура организации

Во главе ООО стоит директор (каб. 32), у которого один заместитель.

Непосредственно руководителю подчиняются:

– канцелярия (каб. 30), в штате: зав. канцелярией и секретарь (в каб. 32 и приемной – пом. 33), зав. архивом (пом. 26);

– служба безопасности (пом. 3, 5, 6), в штате: начальник СБ (каб. 6) и подразделения (группа охраны и режима – ст. инспектор и инспекторы (каб. 6); группа режима КИ – два инспектора (каб. 3); группа ИБ и ТЗИ – один администратор безопасности (каб. 24) и инспектор (каб. 3));

– юрисконсульт (каб. 13);

– проектная группа (каб. 19), в штате: руководитель группы и два инженера 1-й категории;

– группа предпродажной подготовки товара (каб. 20), в штате: руководитель группы, два инженера 2-й категории и два техника;

– отдел автоматизации (IT) (каб. 24), в штате: руководитель отдела, системный администратор и инженер технической поддержки 1-й категории.

Заместитель – по экономике (каб. 32). Ему подчиняются:

– бухгалтерия с кассой (каб. 11), в штате: гл. бухгалтер (каб. 11), экономист, два бухгалтера (каб. 11), кассир (касса);

– отдел маркетинга (каб. 23, 15), в штате: начальник отдела (каб. 15), ст. маркетолог-аналитик, два маркетолога-аналитика, бренд-менеджер (каб. 23);

– отдел логистики, в штате: начальник отдела и два инженера 1-й категории.

Функции начальника отдела кадров выполняет юрисконсульт.

В штате организации находятся также: слесарь-сантехник – 0,5 ставки, электрик – 0,5 ставки, дворник – 0,5 ставки, уборщицы – 1,0 ставки.

В структуре СБ основные задачи структурных подразделений следующие:

– группа охраны и режима: контроль обеспечения охраны объекта со стороны частной охранной организации, контроль работоспособности ОТС, СКУД и СВН, контроль эксплуатационно-технического обслуживания данных систем, обеспечение КПиОР, доставка ценных грузов, проверка почтовых сообщений;

– группа режима КИ: контроль ведения конфиденциального делопроизводства, контроль обеспечения режима КТ, работа с персоналом и посетителями, контроль публикаторской и издательской деятельности, работа со СМИ;

– группа ИБ и ТЗИ: администрирование безопасности ЛВС и ЭВМ, защищенные технологии обработки информации, техническая защита от утечки информации по техническим каналам.

Штатный персонал объекта: общая характеристика (кроме обслуживающего персонала, основных и вспомогательных рабочих)

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
1	Руководство	32/39	Гендиректор/3	39, 41	Высшее техническое профильное	4	4
2	Руководство	32/40	Зам. по экономике/6	40, 41	Высшее техническое профильное	3	3
3	Канцелярия	30/38	Зав. канцелярией/4	38, 41	Среднее специальное	5	3
4	Канцелярия	33/41	Секретарь/9	41, 39, 38	Среднее специальное	6	3
5	Канцелярия	26/42	Зав. архивом	42, 41	Высшее техническое профильное	6	4
6	Служба безопасности	6/2	Начальник СБ/7	2, 3, 4, 5, 6, 36, 7, 1	Высшее военное	7	6
7	Служба безопасности	6/3	Ст. инспектор СБ/4	3, 4, 5, 6, 36, 7	Высшее техническое	7	6
8	Служба безопасности	6/4	Инспектор СБ/6	4, 3	Высшее гуманитарное	6	5
9	Служба безопасности	3/5	Инспектор группы режима КИ/9	5, 6	Высшее гуманитарное	7	6
10	Служба безопасности	3/6	Инспектор группы режима КИ/6	6, 5	Высшее техническое профильное	6	6
11	Служба безопасности	24/36 (29/37)	Администратор безопасности/7	Все (1 – 42)	Высшее техническое профильное	9	9
12	Служба безопасности	3/7	Инспектор СБ (ИБ и ТЗИ)/4	7	Высшее техническое профильное	7	7

Продолжение

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
13	Юрисконсульт	13/21	Юрисконсульт/5	21, 41	Высшее юридическое	4	4
14	Проектная группа	19/22	Руководитель группы/4	22, 23, 24	Высшее техническое	5	5
15	Проектная группа	19/23	Инженер 1-й категории/5	23, 24	Высшее техническое профильное	6	5
16	Проектная группа	19/24	Инженер 1-й категории/5	24, 23	Высшее техническое профильное	6	4
17	Группа предпродажной подготовки товара	20/30	Руководитель группы/4	30, 31, 32	Высшее техническое	7	5
18	Группа предпродажной подготовки товара	20/31	Инженер 2-й категории/8	31, 32	Высшее техническое профильное	6	4
19	Группа предпродажной подготовки товара	20/32	Инженер 2-й категории/12	32, 31	Высшее техническое	7	5
20	Группа предпродажной подготовки товара	20/32	Техник/3	32, 31	Среднее	6	6
21	Группа предпродажной подготовки товара	20/32	Техник/2	32, 31	Среднее специальное	7	6
22	Служба автоматизации (IT)	24/34 (29/37)	Руководитель отдела/3	Все (1 – 42)	Высшее техническое	7	6

Окончание

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
23	Служба автоматизации (IT)	24/35 (29/37)	Системный администратор/6	Все (1 – 42)	Высшее техническое	8	7
24	Служба автоматизации (IT)	24/36 (29/37)	Инженер технической поддержки 1-й категории/8	Все (1 – 42)	Высшее техническое профильное	8	7
25	Бухгалтерия	11/17	Гл. бухгалтер/3	17, 18, 19, 20, 16	Высшее экономическое	7	4
26	Бухгалтерия	11/18	Экономист/5	18, 19, 20, 16	Высшее экономическое	6	5
27	Бухгалтерия	11/19	Бухгалтер/3	19, 20, 16	Высшее экономическое	5	4
28	Бухгалтерия	11/20	Бухгалтер/9	19, 20	Среднее специальное	6	5
29	Бухгалтерия	Касса/ 16	Кассир/6	16, 19	Среднее специальное	3	1
30	Отдел маркетинга	15/29	Начальник отдела маркетинга/3	29, 25, 26, 27, 28	Высшее экономическое	7	4
31	Отдел маркетинга	23/25	Ст. маркетолог-аналитик/14	25, 26	Высшее экономическое	6	4
32	Отдел маркетинга	23/26	Маркетолог-аналитик/7	26, 25	Высшее экономическое	6	4
33	Отдел маркетинга	23/27	Маркетолог-аналитик/3	27, 28	Среднее специальное	4	4
34	Отдел маркетинга	23/28	Бренд-менеджер/3	28, 27	Высшее экономическое	5	5
35	Отдел логистики	9/13	Начальник отдела/4	13, 14, 15	Высшее экономическое	6	5
36	Отдел логистики	9/14	Инженер 1-й категории/3	14, 15	Высшее гуманитарное	5	5
37	Отдел логистики	9/15	Инженер 1-й категории/8	15, 14	Высшее техническое	4	3

Структура защищаемой информации

№ п\п	Наименование источника информации	Гриф	Источник информации	Место нахождения источника информации
1	Структура предприятия	КТ	Контракты, документы на бумажных носителях, персонал фирмы	Сейф с документами, каб. 9; ПК 13
2	Личные сведения о сотрудниках фирмы	ПДн	Документы на бумажных и электронных носителях, БД, персонал фирмы, бухгалтерия	Сейф с документами, касса; ПК 41, 38, 39, 16
3	Учредительные документы	К	Устав организации, бумажные документы	Рабочий стол в кабинете директора, секретаря; ПК 38, 39, 41, 17
4	Сведения о кредитах, контрактах	СК	Документы на бумажных и электронных носителях, БД, гл. бухгалтер	Сейф с документами, каб. 9; ПК 13
5	База данных заказчиков, партнеров фирмы	К	Документы на бумажных и электронных носителях, гл. бухгалтер, стол директора	Сейф с документами, каб. 9; ПК 13
6	Сведения о конкурентах (в том числе компромат)	КТ	Документы на бумажных и электронных носителях, гл. бухгалтер, стол директора	Сейф с документами, каб. 9; ПК 13
7	Пароли к используемому ПО и web-сайтам	КТ	Документы на электронных носителях, СБ, отдел IT	ПК 2, 34, 35, 36
8	Сведения о концепте и продвижении продукции	КТ	Документы на бумажных и электронных носителях, отдел маркетинга	Сейф с документами, каб. 9; ПК 13
9	Методы и способы производства, новые технологии	К	Документы на бумажных и электронных носителях, отдел маркетинга	Сейф с документами, каб. 9; ПК 13
10	Конкурентоспособность производимой продукции, эффективность экспорта и импорта, предполагаемое время выхода на рынок	СК	Документы на бумажных и электронных носителях, отдел маркетинга	Сейф с документами, каб. 9; ПК 13

Окончание

№ п\п	Наименование источника информации	Гриф	Источник информации	Место нахождения источника информации
11	Планы и характер рекламной и публикаторской деятельности	КТ	Документы на бумажных и электронных носителях, юрисконсульты	Сейф с документами, каб. 9; ПК 13
12	Кадровый состав и его формирование	СК	Документы на бумажных и электронных носителях, бухгалтерия, ОК, стол директора	Сейф с документами, каб. 9; ПК 13
13	Сведения о системе безопасности организации	КТ	Документы на бумажных и электронных носителях, СБ, рабочий стол директора	Сейф с документами, каб. 9; ПК 13
14	Телефонные переговоры сотрудников и клиентов	КТ	Документы на электронных носителях, СБ, отдел IT	Сейф с документами, каб. 9; ПК 13

Вариант № 3

Объект – государственная регистрационная организация (например, кадастровая палата, название придумать самостоятельно), занимающая часть 3-го этажа трехэтажного кирпичного административного здания с подвалом и дневным постом охраны. Организация осуществляет прием посетителей, в помещениях всегда многолюдно. В здании подвал, первые два этажа и смежные помещения занимают (арендуют) прочие «не охраняемые» собственники.

Перекрытия полов и потолков капитальные, из железобетонных панелей. Имеется деревянный люк на плоскую крышу, чердака нет. Все внутренние двери деревянные, филенчатые, полнотелые. Двери в служебные кабинеты и бухгалтерию, кассу, архив, канцелярию, серверную, пост охраны и другие имеют по одному врезному замку. Двери в холлах, коридорах, тамбурах остекленные в верхней половине двери и запорных устройств не имеют. Все внутренние перегородки и стены (кроме наружных по периметру здания) гипсокартонные, каркасные или в кирпич (полкирпича), не капитальные. Во всех служебных каби-

нетах имеются персональные компьютеры, на складах – дорогостоящие материальные ценности. В помещениях 2 и кассы установлены сейфы массой 150 – 200 кг без крепления к полу и стенам. Кабинет 2 – защищаемое режимное помещение с хранением информации, составляющей служебную тайну.

Двери:

Д1 – дверь пластиковая, полнотелая, с одним врезным замком

Решетчатые раздвижные двери в помещениях отсутствуют.

Окна:

О1 – окно пластиковое, с двойным остеклением, без защитных пленок, решетка со стороны помещения из прутка D = 16 мм, размер ячейки 120×150 мм

О2 – окно с деревянными рамами, двойным остеклением, без защитных пленок, решетки отсутствуют

Экспликация помещений объекта:

1 – приемная; 1а – кабинет начальника; 2 – канцелярия; 3 – 5 – служебные кабинеты; 6 – служебный кабинет; 6а – склад; 6б – архив; 7 – служебные кабинеты; 7а – отдел кадров; 8 – бухгалтерия; 9 – 10 – служебный кабинет; 11 – пост охраны; 12 – коридор; 13 – лестничная клетка; 14 – санузлы; 15 – служебный кабинет; 16 – серверная.

Структура организации

Во главе организации стоит директор (каб. 1а).

В штате организации:

– канцелярия (каб. 38), в штате: зав. канцелярией и два секретаря (один – в каб. 15 и один – в приемной (каб. 1)), зав. архивом (пом. 6б);

– служба безопасности (пом. 2, 7), в штате: начальник СБ (каб. 2) и подразделения (группа охраны и режима – ст. инспектор и инспектор (каб. 2); группа режима «для служебного пользования» (ДСП) – один инспектор (каб. 7); группа ИБ и ТЗИ – один администратор безопасности (каб. 7), ст. инспектор и инспектор (каб. 7), ст. юрисконсульт по безопасности (каб. 3));

– бухгалтерия с кассой (каб. 8), в штате: гл. бухгалтер (каб. 8), экономист, два бухгалтера, кассир;

– служба автоматизации (IT) (каб. 10), в штате: системный администратор и два инженера технической поддержки 1-й категории;

– отдел кадров (каб. 7а), в штате: ст. инспектор ОК;

– 1-й отдел (каб. 4), в штате: начальник отдела, гл. специалист, ст. специалист, два инженера 1-й категории;

– 2-й отдел (каб. 3), в штате: начальник отдела, гл. специалист, ст. специалист (все занимают каб. 3), четыре инженера 1-й категории (каб. 5);

– 3-й отдел (каб. 3), в штате: начальник отдела, два инженера 1-й категории (каб. 6);

– 4-й отдел (каб. 9), в штате: начальник отдела, зам. начальника отдела, гл. специалист, ст. специалист, два инженера 1-й категории.

В подчинении начальнику отдела кадров находятся: кладовщик (каб. 6а), слесарь-сантехник – 0,5 ставки, электрик – 0,5 ставки, дворник – 0,5 ставки, уборщицы – 1,5 ставки.

В структуре СБ основные задачи структурных подразделений следующие:

– группа охраны и режима: контроль обеспечения охраны объекта со стороны частной охранной организации, контроль работоспособности ОТС, СКУД и СВН, контроль эксплуатационно-технического обслуживания данных систем, обеспечение КПиОР, доставка ценных грузов, проверка почтовых сообщений;

– группа режима ДСП: контроль ведения делопроизводства ДСП, работа с персоналом и посетителями, контроль публикаторской и издательской деятельности, работа со СМИ, контроль обеспечения режима КТ;

– группа ИБ и ТЗИ: администрирование безопасности ЛВС и ЭВМ, защищенные технологии обработки информации, техническая защита от утечки информации по техническим каналам;

– юрисконсульт по безопасности: юридическое сопровождение обеспечения безопасности, организационное обеспечение ИБ, аналитическая работа.

Штатный персонал объекта: общая характеристика (кроме обслуживающего персонала, основных и вспомогательных рабочих)

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
1	Руководство	1а/2	Директор/3	2	Высшее техническое профильное	7	7
2	Канцелярия	15/42	Зав. канцелярией/5	42, 1, 43	Высшее техническое	6	5
3	Канцелярия	15/43	Секретарь/3	42, 1, 43	Высшее техническое	5	4
4	Канцелярия	1/1	Секретарь/4	1, 2	Высшее гуманитарное	5	4
5	Канцелярия	6б/26	Зав. архивом/12	26, 43	Высшее гуманитарное	6	4
6	Служба безопасности	2/4	Начальник СБ/5	4, 3, 5, 6, 27, 29, 30, 7	Высшее военное	8	7
7	Служба безопасности	2/5	Ст. инспектор СБ/4	5, 6	Высшее техническое профильное	8	7
8	Служба безопасности	2/6	Инспектор СБ/6	6, 5	Высшее гуманитарное	7	6
9	Служба безопасности	7/27	Инспектор группы режима ДСП/4	27, 42	Высшее техническое профильное	7	6
10	Служба безопасности	10/47 (16/44)	Администратор безопасности/3	Все (1 – 47)	Высшее техническое профильное	10	10

Продолжение

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
11	Служба безопасности	7/29	Ст.инспектор СБ (ИБ и ТЗИ)/1	29, 30	Высшее техническое профильное	6	6
12	Служба безопасности	7/30	Инспектор СБ (ИБ и ТЗИ)/5	30, 29	Высшее военное	6	5
13	Служба безопасности	3/7	Ст. юрисконсульт/6	7	Высшее юридическое	5	5
14	Бухгалтерия	8/37	Гл. бухгалтер/3	37, 38, 39, 40	Высшее экономическое	4	4
15	Бухгалтерия	8/38	Экономист/6	38, 39, 40, 41	Высшее экономическое	4	4
16	Бухгалтерия	8/39	Бухгалтер/8	39, 40	Высшее экономическое	4	3
17	Бухгалтерия	8/40	Бухгалтер/4	40, 39, 41	Среднее специальное	3	3
18	Бухгалтерия	Касса/41	Кассир/12	41	Среднее специальное	2	2
19	Служба автоматизации (IT)	10/45 (16/44)	Системный администратор/5	Все (1 – 47)	Высшее военное	9	7
20	Служба автоматизации (IT)	10/46 (16/44)	Инженер технической поддержки 1-й категории/8	Все (1 – 47)	Высшее техническое	9	7

Продолжение

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
21	Служба автоматизации (IT)	10/46	Инженер технической поддержки 1-й категории/4	Все (1 – 47)	Высшее техническое	9	7
22	Отдел кадров	7а/28	Ст. инспектор ОК/4	28	Высшее техническое	8	6
23	1-й отдел	4/15	Начальник отдела/5	15, 16, 17, 18, 19	Высшее экономическое	8	6
24	1-й отдел	4/16	Гл. специалист/7	16, 17	Высшее техническое	7	4
25	1-й отдел	4/17	Ст. специалист/8	17, 16	Высшее техническое профильное	6	5
26	1-й отдел	4/18	Инженер 1-й категории/3	18, 19	Высшее техническое профильное	6	4
27	1-й отдел	4/19	Инженер 1-й категории/8	19, 18	Высшее техническое	6	4
28	2-й отдел	3/10	Начальник отдела/3	10, 9, 8, 11, 12, 13, 14	Высшее гуманитарное	5	4
29	2-й отдел	3/9	Гл. специалист/6	9, 8	Высшее техническое	5	4
30	2-й отдел	3/8	Ст. специалист/4	8, 9	Высшее техническое профильное	5	4

Продолжение

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
31	2-й отдел	5/11	Инженер 1-й категории/6	11, 12	Высшее техническое профильное	4	4
32	2-й отдел	5/12	Инженер 1-й категории/7	12, 11	Высшее экономическое	5	4
33	2-й отдел	5/13	Инженер 1-й категории/8	13, 14	Высшее техническое профильное	4	3
34	2-й отдел	5/14	Инженер 1-й категории/10	14, 13	Высшее экономическое	6	4
35	3-й отдел	6/20	Начальник отдела/3	20, 21, 22, 23, 24	Высшее техническое	4	4
36	3-й отдел	6/21	Инженер 1-й категории/5	21, 22	Высшее экономическое	4	4
37	3-й отдел	6/22	Инженер 1-й категории/2	22, 21	Высшее техническое	6	5
38	3-й отдел	6/23	Инженер 1-й категории/8	23, 24	Высшее экономическое	3	2
39	3-й отдел	6/24	Инженер 1-й категории/12	24, 23	Высшее военное	5	4
40	4-й отдел	9/31	Начальник отдела/4	31, 32, 33, 34, 35, 36	Высшее гуманитарное	5	4
41	4-й отдел	9/32	Зам. начальника отдела/7	32, 31, 33	Высшее гуманитарное	4	3

Окончание

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
42	4-й отдел	9/33	Гл. специалист/9	33, 32, 34	Высшее техническое	4	4
43	4-й отдел	9/34	Ст. специалист/12	34, 35	Высшее военное	3	3
44	4-й отдел	9/35	Инженер 1-й категории/13	35, 34	Высшее техническое профильное	5	4
45	4-й отдел	9/36	Инженер 1-й категории/14	36, 34, 35	Высшее военное	3	3
46	Кладовщик	6а/25	Кладовщик/3	25, 31, 32	Высшее военное	4	2

Структура защищаемой информации

№ п\п	Наименование источника информации	Гриф	Источник информации	Место нахождения источника информации
1	Структура предприятия	К	Контракты, документы на бумажных носителях, персонал	Сейф с документами, каб. 2; ПК 5
2	Личные сведения о сотрудниках	ПДн	Документы на бумажных и электронных носителях, БД, персонал	Сейф с документами, каб. 2; ПК 5
3	Учредительные документы	К	Устав организации, бумажные документы	Рабочий стол в кабинете директора, сейф с документами, каб. 2; ПК 5
4	База данных клиентов, партнеров	ДСП	Документы на бумажных и электронных носителях, гл. бухгалтер	Сейф с документами, каб. 15; ПК 1, 2, 37, 41
5	Пароли к используемому ПО и web-сайтам	ДСП	Документы на электронных носителях, СБ, отдел IT	ПК 45, 47

Окончание

№ п\п	Наименование источника информации	Гриф	Источник информации	Место нахождения источника информации
6	Архив различных версий разрабатываемых ПО, web-сайтов	СК	Документы на электронных носителях, СБ, отдел IT	ПК 45, 47, 26
7	Регистрационные БД клиентов	ДСП	Документы на бумажных и электронных носителях	Сейф с документами, каб. 2; ПК 5
8	Методы и способы производства, новые технологии	ДСП	Документы на бумажных и электронных носителях	Сейф с документами, каб. 2; ПК 42, 43
9	Планы по реорганизации и развитию деятельности организации	ДСП	Документы на бумажных и электронных носителях	Сейф с документами, каб. 2; ПК 1, 2, 37, 27
10	Планы и характер рекламной и публикаторской деятельности	ДСП	Документы на бумажных и электронных носителях, юрисконсульты	Сейф с документами, каб. 2; ПК 7
11	Кадровый состав и его формирование	СК	Документы на бумажных и электронных носителях, бухгалтерия, ОК, стол директора	Сейф с документами, каб. 2; ПК 7, 28
12	Сведения о системе безопасности организации	ДСП	Документы на бумажных и электронных носителях, СБ, рабочий стол директора	Сейф с документами, каб. 2; ПК 1, 4
13	Телефонные переговоры сотрудников и клиентов	ДСП	Документы на электронных носителях, СБ, отдел IT	ПК 4, 27
14	Направления модернизации известных технологий, процессов и оборудования	ДСП	Документы на бумажных и электронных носителях	Сейф с документами, каб. 2; ПК 5, 2, 27

Вариант № 4

Объект – государственная правоохранительная организация (название придумать самостоятельно), занимающая одноэтажное кирпичное административное здание с подвалом и круглосуточным постом охраны.

Перекрытия полов и потолков капитальные, из железобетонных панелей. Имеется деревянный люк на неэксплуатируемый чердак. Все внутренние двери (за исключением обозначенных) деревянные, филенчатые, полнотелые. Двери в служебные кабинеты и бухгалтерию, архив, серверную, пост охраны и другие имеют по одному врезному замку. Двери в холлах, коридорах, тамбурах остекленные в верхней половине двери и запорных устройств не имеют. Все внутренние перегородки и стены (кроме наружных по периметру здания) гипсокартонные, каркасные или в кирпич (полкирпича), не капитальные. Во всех служебных кабинетах имеются персональные компьютеры, на складах – дорогостоящие материальные ценности. В помещениях 2 и кассы установлены сейфы массой 150 – 200 кг без крепления к полу и стенам. Кабинет 13 – защищаемое режимное помещение с хранением информации, составляющей служебную тайну.

Двери:

Д1 – дверь цельнометаллическая, с двумя врезными замками на расстоянии более 300 мм

Д2 – дверь цельнометаллическая, с одним врезным замком

Д3 – дверь решетчатая, раздвижная, с одним врезным замком

Д4 – дверь полнотелая, деревянная, филенчатая, обитая с наружной стороны железом толщиной 1 мм с загибом на торец, с двумя врезными замками на расстоянии менее 300 мм

Окна:

О1 – окно пластиковое, с двойным остеклением, без защитных пленок, решетка со стороны улицы из прутка D = 16 мм, размер ячейки 150×150 мм

О2 – окно пластиковое, с двойным остеклением, без защитных пленок, решетки отсутствуют

О3 – окно пластиковое, с двойным остеклением, без защитных пленок, решетка со стороны помещения из прутка D = 16 мм, размер ячейки 120×150 мм

Экспликация помещений объекта

ПОДВАЛ: 1 – архив; 2 – серверная; 3 – техническое помещение; 4 – коридор; 5 – техническое помещение; 6 – душевые и санузлы; 7 – 8 – склады; 9 – коридор; 10 – актовый зал; 11 – 12 – служебные кабинеты

1-й ЭТАЖ: 1, 3 – 4 – служебные кабинеты; 2 – служебный кабинет; 5 – дежурная часть, пост охраны; 6 – фойе; 7 – коридор; 8 – приемная; 8а – кабинет начальника; 9 – комната заряжания; 10 – комната хранения оружия; 11 – служебный кабинет; 12 – бухгалтерия; 13 – канцелярия; 14 – 15 – служебные кабинеты.

Структура организации

Во главе организации стоит начальник (каб. 8а), у которого два заместителя по службе и технике.

Непосредственно начальнику подчиняются:

– канцелярия (каб. 2), в штате: зав. канцелярией и два секретаря (каб. 8);

– служба безопасности (пом. 13, 15), в штате: начальник СБ (каб. 5) и подразделения (группа охраны и режима – ст. инспектор и инспектор (каб. 13); группа режима ДСП – один инспектор (каб. 15); группа ИБ и ТЗИ – один администратор безопасности (каб. 14), ст. инспектор (каб. 15), ст. юрисконсульт (каб.8));

– бухгалтерия с кассой (каб. 12), в штате: гл. бухгалтер, экономист, бухгалтер, кассир (касса).

Заместителю начальника по службе подчиняются:

– отдел кадров, аналитической и оргштатной работы (каб. 12), в штате: нач. отдела, ст. инспектор ОК, инспектор оргштатной работы;

– отдел службы (каб. 8, 11), в штате: начальник отдела (он же – заместитель начальника по службе) (каб. 8), ст. инспектор, инспектор (каб. 8); ст. инспектор и два инспектора (каб. 11);

– дежурная часть – три старших смены и четыре дежурных (каб. 5);

– отдел материально-технического обеспечения, в штате: начальник отдела (каб. 1), ст. инспектор, инспектор (каб. 1).

Заместителю начальника по технике подчиняются:

– отдел техники (каб. 3, 4), в штате: начальник отдела (он же – заместитель начальника по технике) (каб. 3), ст. инспектор-инженер, инспектор-инженер (каб. 3); гл. специалист и два инспектора-инженера (каб. 4);

– группа автоматизации (IT) – системный администратор и инспектор-инженер по техподдержке (каб. 14);

– кладовщик (каб. 7, 8).

В подчинении начальнику отдела кадров находятся: слесарь-сантехник – 0,5 ставки, электрик – 0,5 ставки, дворник – 0,5 ставки, уборщицы – 1,5 ставки.

В структуре СБ основные задачи структурных подразделений следующие:

– группа охраны и режима: контроль обеспечения охраны объекта собственными силами, контроль работоспособности ОТС, СКУД и СВН, контроль эксплуатационно-технического обслуживания данных систем, обеспечение КПиОР, доставка ценных грузов, проверка почтовых сообщений;

– группа режима КИ: контроль ведения ДСП делопроизводства, работа с персоналом и посетителями, контроль публикаторской и издательской деятельности, работа со СМИ, контроль обеспечения режима конфиденциальности;

– группа ИБ и ТЗИ: администрирование безопасности ЛВС и ЭВМ, защищенные технологии обработки информации, техническая защита от утечки информации по техническим каналам;

– юрисконсульт по безопасности: юридическое сопровождение обеспечения безопасности, организационное обеспечение ИБ, аналитическая работа.

Штатный персонал объекта: общая характеристика (кроме обслуживающего персонала, основных и вспомогательных рабочих)

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
1	Руководство	8а/27	Начальник/12	27, 29	Высшее техническое профильное	5	3
2	Канцелярия	2/17; 1/1	Зав. канцелярией/15	17, 1, 18, 29	Высшее гуманитарное	6	5
3	Канцелярия	2/18	Секретарь/12	18, 28, 1	Среднее специальное	6	5
4	Канцелярия	8/29	Секретарь/14	29, 27	Высшее гуманитарное	4	2

Продолжение

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
5	Служба безопасности	5/25	Начальник СБ/13	25, 39, 40, 41, 38, 42, 26	Высшее военное	8	7
6	Служба безопасности	13/39	Ст. инспектор СБ/11	39, 40, 26	Высшее техническое профильное	8	7
7	Служба безопасности	13/40	Инспектор СБ/10	40, 39, 26	Высшее гуманитарное	7	7
8	Служба безопасности	15/41	Инспектор группы режима ДСП/5	41, 40, 17, 1, 29	Высшее техническое	8	7
9	Служба безопасности	14/38	Администратор безопасности/7	Все (1 – 42)	Высшее техническое профильное	10	9
10	Служба безопасности	15/42	Ст. инспектор СБ (ИБ и ТЗИ)/8	42, 38	Высшее техническое	6	6
11	Служба безопасности	8/28	Ст. юрисконсульт/4	28	Высшее военное	5	5
12	Бухгалтерия	12/30	Гл. бухгалтер/9	30, 31, 32, 33	Высшее экономическое	5	4
13	Бухгалтерия	12/31	Экономист/6	31, 32, 33	Высшее экономическое	4	3
14	Бухгалтерия	12/32	Бухгалтер/7	32, 33	Высшее экономическое	4	3
15	Бухгалтерия	Касса/33	Кассир/3	33, 32	Среднее специальное	3	2

Продолжение

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
16	Отдел кадров, аналитической и оргштатной работы	12/11	Начальник отдела/3	11, 12, 13	Высшее техническое профильное	6	4
17	Отдел кадров, аналитической и оргштатной работы	12/12	Ст. инспектор ОК/6	12, 13	Высшее техническое	5	2
18	Отдел кадров, аналитической и оргштатной работы	12/13	Инспектор оргштатной работы/4	13, 12	Высшее военное	7	5
19	Отдел службы	8/4	Начальник отдела/3	4, 5, 6, 7, 8, 9	Высшее гуманитарное	5	4
20	Отдел службы	8/5	Ст. инспектор/5	5, 6	Высшее военное	4	4
21	Отдел службы	8/6	Инспектор/4	6, 5	Высшее техническое профильное	5	3
22	Отдел службы	11/7	Ст. инспектор/8	7, 8	Высшее гуманитарное	4	2
23	Отдел службы	11/8	Инспектор/2	8, 9	Высшее техническое	3	3
24	Отдел службы	11/9	Инспектор/9	9, 11	Высшее техническое профильное	5	4
25	Дежурная часть	5/26	Ст. смены/4	26	Высшее гуманитарное	6	4
26	Дежурная часть	5/26	Ст. смены/7	26	Высшее гуманитарное	4	3

Продолжение

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
27	Дежурная часть	5/26	Ст. смены/3	26	Высшее гуманитарное	5	4
28	Дежурная часть	5/26	Инспектор-дежурный/6	26	Высшее военное	6	3
29	Дежурная часть	5/26	Инспектор-дежурный/7	26	Высшее техническое профильное	4	4
30	Дежурная часть	5/26	Инспектор-дежурный/8	26	Высшее гуманитарное	3	3
31	Дежурная часть	5/26	Инспектор-дежурный/3	26	Высшее гуманитарное	6	4
32	Отдел ОМТиХО	1/14	Начальник отдела/5	14, 15, 16	Высшее гуманитарное	7	6
33	Отдел ОМТиХО	1/15	Ст. инспектор/9	15, 16	Высшее гуманитарное	5	5
34	Отдел ОМТиХО	1/16	Инспектор/14	16, 15	Высшее техническое профильное	4	3
35	Отдел техники	3/19	Начальник отдела/3	19, 20, 21, 22, 23, 24	Высшее техническое профильное	7	4
36	Отдел техники	3/20	Ст. инспектор-инженер/5	20, 21, 22	Высшее военное	7	4
37	Отдел техники	3/21	Инспектор-инженер/4	21, 20, 22	Высшее техническое профильное	6	3

Окончание

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
38	Отдел техники	4/22	Гл. специалист/5	22, 21	Высшее военное	7	4
39	Отдел техники	4/23	Инспектор-инженер/3	23, 24	Высшее техническое профильное	6	5
40	Отдел техники	4/24	Инспектор-инженер/1	24, 23	Высшее техническое профильное	7	5
41	Служба автоматизации (IT)	14/37	Системный администратор/7	Все (1 – 42)	Высшее техническое	10	8
42	Служба автоматизации (IT)	14/37	Инженер технической поддержки 1-й категории/3	Все (1 – 42)	Высшее техническое профильное	9	7
43	Кладовщик	7/3	Кладовщик	7/3	Высшее военное	3	2

Структура защищаемой информации

№ п\п	Наименование источника информации	Гриф	Источник информации	Место нахождения источника информации
1	Структура предприятия	К	Контракты, документы на бумажных носителях, персонал	Сейф с документами, каб. 13; ПК 39, 28, 27, 28, 29
2	Личные сведения о сотрудниках	ПДн	Документы на бумажных и электронных носителях, БД, персонал	Сейф с документами, каб. 2; сейф в кассе; ПК 27, 39, 30, 26

Продолжение

№ п\п	Наименование источника информации	Гриф	Источник информации	Место нахождения источника информации
3	Учредительные документы	ДСП	Нормативно-регламентирующие документы на бумажных и электронных носителях	Рабочий стол в кабинете начальника, сейф с документами, каб. 13; ПК 27, 39, 30, 26
4	База данных контрагентов	ДСП	Документы на бумажных и электронных носителях, гл. бухгалтер	Сейф с документами, каб. 13; ПК 27, 39, 30, 28
5	Пароли к используемому ПО и web-сайтам	ДСП	Документы на электронных носителях, СБ, отдел IT	ПК 37, 38
6	Архив различных версий специализированного ПО, web-сайтов	СК	Документы на электронных носителях, СБ, отдел IT	ПК 37, 38
7	Регистрационные БД клиентов	ДСП	Документы на бумажных и электронных носителях	Сейф с документами, каб. 13; ПК 27, 39, 30
8	Методы и способы производства, новые технологии	ДСП	Документы на бумажных и электронных носителях	Сейф с документами, каб. 13; ПК 39, 27
9	Планы по реорганизации и развитию деятельности организации	ДСП	Документы на бумажных и электронных носителях	Сейф с документами, каб. 13; ПК 39, 27
10	Планы и характер рекламной и публикаторской деятельности	ДСП	Документы на бумажных и электронных носителях, юрисконсульты	Сейф с документами, каб. 13; ПК 27, 28
11	Кадровый состав и его формирование	СК	Документы на бумажных и электронных носителях, бухгалтерия, ОК, стол начальника	Сейф с документами, каб. 13; ПК 11, 27, 28

Окончание

№ п\п	Наименование источника информации	Гриф	Источник информации	Место нахождения источника информации
12	Сведения о системе безопасности организации	ДСП	Документы на бумажных и электронных носителях, СБ, рабочий стол начальника	Сейф с документами, каб. 13; ПК 25, 26
13	Телефонные переговоры сотрудников и клиентов	ДСП	Документы на электронных носителях, СБ, отдел IT	ПК 25, 26
14	Направления модернизации известных технологий, процессов и оборудования	ДСП	Документы на бумажных и электронных носителях	Сейф с документами, каб. 13; ПК 27, 39

Вариант № 5

Объект – государственная организация (например, местная администрация, название придумать самостоятельно), занимающая 1-й этаж трехэтажного кирпичного здания с дневным постом охраны на 1-м этаже. Подвал в здании отсутствует. В здании 2-й и 3-й этажи занимают (арендуют) прочие «не охраняемые» собственники.

Перекрытия полов и потолков капитальные, из железобетонных панелей. Все внутренние двери деревянные, филенчатые, полнотелые. Двери в служебные кабинеты и бухгалтерию, кассу, архив, канцелярию, серверную и другие имеют по одному врезному замку. Двери в холлах, коридорах, тамбурах остекленные в верхней половине двери и запорных устройств не имеют. Все внутренние перегородки и стены (кроме наружных по периметру здания) гипсокартонные, каркасные или в кирпич (полкирпича), не капитальные. Во всех служебных кабинетах имеются персональные компьютеры, на складе – дорогостоящие материальные ценности. В помещениях 3 и кассы установлены сейфы массой 150 – 200 кг без крепления к полу и стенам. Кабинет 3 – защищаемое выделенное помещение с хранением информации, составляющей служебную тайну.

Двери:

Д1 – дверь цельнометаллическая, с одним врезным замком

Д2 – дверь пластиковая, полнотелая, с одним врезным замком

Окна:

О1 – окно пластиковое, с двойным остеклением, без защитных пленок, решетки отсутствуют

О2 – окно пластиковое, с двойным остеклением, без защитных пленок, решетка со стороны помещения из прутка D = 16 мм, размер ячейки 200×200 мм

О3 – окно пластиковое, с двойным остеклением, без защитных пленок, решетка со стороны помещения из прутка D = 16 мм, размер ячейки 120×150 мм

Экспликация помещений объекта:

1 – 2; 4 – 8 – служебные кабинеты; 3 – канцелярия; 9 – архив; 10 – серверная; 11 – холл; 12 – служебный кабинет; 13 – приемная; 13а – кабинет начальника; 14 – склад; 15 – 16 – служебные кабинеты; 17 – бухгалтерия; 18 – касса; 19 – служебный кабинет.

Структура организации

Во главе организации стоит директор (каб. 13а).

В штате организации:

– канцелярия (каб. 7), в штате: зав. канцелярией и два секретаря (один – в каб. 7 и один – в приемной (каб. 13)), зав. архивом (пом. 9);

– служба безопасности (пом. 15, 16), в штате: начальник СБ (каб. 15) и подразделения (группа охраны и режима – ст. инспектор (каб. 15); группа режима ДСП – один инспектор (каб. 16); группа ИБ и ТЗИ – один администратор безопасности (каб. 16), ст. инспектор и инспектор (каб. 16), ст. юрисконсульт по безопасности (каб. 19));

– бухгалтерия с кассой (каб. 17), в штате: гл. бухгалтер (каб. 17), экономист, два бухгалтера, кассир;

– служба автоматизации (IT) (каб. 12), в штате: системный администратор и инженер технической поддержки 1-й категории;

– отдел кадров и юрисконсульт (каб. 19), в штате: ст. инспектор ОК и юрисконсульт;

– 1-й отдел (каб. 1, 2), в штате: начальник отдела, гл. специалист, ст. специалист (каб. 1), два инженера 1-й категории (каб. 2);

– 2-й отдел (каб. 3, 4), в штате: начальник отдела, гл. специалист, ст. специалист (все занимают каб. 3), три инспектора 1-й категории (каб. 3);

– 3-й отдел (каб. 5, 6, 7), в штате: начальник отдела, зам. начальника отдела, гл. специалист (каб. 5), ст. специалист, инженер 1-й категории (каб. 6), три инженера 1-й категории (каб. 7).

Кладовщик (каб. 14) находится в подчинении начальнику 1-го отдела.

В подчинении начальнику 3-го отдела находятся зав. гаражом и три водителя.

В подчинении начальнику отдела кадров находятся: кладовщик (каб. 6а), слесарь-сантехник – 0,5 ставки, электрик – 0,5 ставки, дворник – 0,5 ставки, уборщица – 1,0 ставки.

В структуре СБ основные задачи структурных подразделений следующие:

– группа охраны и режима: контроль обеспечения охраны объекта со стороны частной охранной организации, контроль работоспособности ОТС, СКУД и СВН, контроль эксплуатационно-технического обслуживания данных систем, обеспечение КПиОР, доставка ценных грузов, проверка почтовых сообщений;

– группа режима ДСП: контроль ведения ДСП делопроизводства, работа с персоналом и посетителями, контроль публикаторской и издательской деятельности, работа со СМИ, контроль обеспечения режима КТ;

– группа ИБ и ТЗИ: администрирование безопасности ЛВС и ЭВМ, защищенные технологии обработки информации, техническая защита от утечки информации по техническим каналам;

– юрисконсульт по безопасности: юридическое сопровождение обеспечения безопасности, организационное обеспечение ИБ, аналитическая работа.

Штатный персонал объекта: общая характеристика
(кроме обслуживающего персонала, основных
и вспомогательных рабочих)

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
1	Руководство	13а/33	Директор/5	33	Высшее гуманитарное профильное	8	6
2	Канцелярия	8/17	Зав. канцелярией/7	17, 18, 32, 22	Высшее гуманитарное	7	6

Продолжение

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
3	Канцелярия	8/18	Секретарь/6	18, 32	Высшее техническое	7	5
4	Канцелярия	13/32	Секретарь/5	32, 18	Высшее гуманитарное	6	4
5	Канцелярия	9/22	Зав. архивом/3	22, 18	Высшее гуманитарное	4	3
6	Служба безопасности	15/37	Начальник СБ/5	37, 38, 42, 41, 40, 34	Высшее техническое профильное	8	8
7	Служба безопасности	15/38	Ст. инспектор СБ/6	38	Высшее техническое	7	6
8	Служба безопасности	16/42	Инспектор группы режима ДСП/11	42, 17, 18, 32, 22	Высшее техническое профильное	8	7
9	Служба безопасности	16/41 (10/24)	Администратор безопасности/6	Все (1 – 42)	Высшее техническое	10	9
10	Служба безопасности	16/40	Ст. инспектор СБ (ИБ и ТЗИ)/1	40	Высшее техническое профильное	8	8
11	Служба безопасности	19/34	Ст. юрисконсульт/7	34	Высшее юридическое	5	5
12	Бухгалтерия	17/25	Гл. бухгалтер/13	25, 26, 27, 28, 29	Высшее экономическое	6	5

Продолжение

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
13	Бухгалтерия	17/26	Экономист/7	26, 27, 28, 29	Высшее экономическое	4	4
14	Бухгалтерия	17/27	Бухгалтер/9	27, 28, 29	Высшее экономическое	4	4
15	Бухгалтерия	17/28	Бухгалтер/11	28, 27, 29	Высшее экономическое	3	3
16	Бухгалтерия	18/29	Кассир/13	29, 27	Среднее специальное	2	1
17	Служба автоматизации (IT)	12/30 (10/24)	Системный администратор/15	Все (1 – 42)	Высшее техническое	9	8
18	Служба автоматизации (IT)	12/31	Инженер технической поддержки 1-й категории/9	Все (1 – 42)	Высшее юридическое	9	6
19	Отдел кадров	19/35	Ст. инспектор отдела кадров/4	35, 36	Высшее техническое	7	5
20	Юрисконсульт	19/36	Юрисконсульт/17	36, 35	Высшее юридическое	5	3
21	1-й отдел	1/4	Начальник отдела/5	4, 5, 6, 9, 10	Высшее экономическое	4	4
22	1-й отдел	1/5	Гл. специалист/6	5, 6	Высшее техническое	6	5

Продолжение

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
23	1-й отдел	1/6	Ст. специалист/12	6, 5	Высшее техническое профильное	4	4
24	1-й отдел	2/9	Инженер 1-й категории/13	9, 10	Высшее техническое	7	4
25	1-й отдел	2/10	Инженер 1-й категории/12	10, 9	Высшее техническое	4	3
26	2-й отдел	3/14	Начальник отдела/13	14, 15, 16, 19, 20, 21	Высшее гуманитарное	3	3
27	2-й отдел	3/15	Гл. специалист/16	15, 16, 19	Высшее техническое	7	5
28	2-й отдел	3/16	Ст. специалист/14	16, 15	Высшее техническое профильное	4	4
29	2-й отдел	4/19	Инспектор 1-й категории/13	19, 20	Высшее гуманитарное	3	3
30	2-й отдел	4/20	Инспектор 1-й категории/15	20, 19	Высшее экономическое	4	2
31	2-й отдел	4/21	Инспектор 1-й категории/9	21, 20	Высшее гуманитарное	5	4
32	3-й отдел	5/1	Начальник отдела/3	1, 2, 3, 8, 7, 11, 12, 13	Высшее техническое	5	4

Окончание

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
33	3-й отдел	5/2	Зам. начальника отдела/5	2, 3, 8, 7, 11	Высшее экономическое	3	3
34	3-й отдел	5/3	Гл. специалист/2	3, 8, 11, 12	Высшее техническое	6	4
35	3-й отдел	6/8	Ст. специалист/8	8, 7	Высшее экономическое	5	4
36	3-й отдел	6/7	Инженер 1-й категории/10	7, 8	Высшее военное	4	4
37	3-й отдел	7/11	Инженер 1-й категории/17	11, 12	Высшее гуманитарное	4	4
38	3-й отдел	7/12	Инженер 1-й категории/7	12, 11, 13	Высшее гуманитарное	3	3
39	3-й отдел	7/13	Инженер 1-й категории/4	13, 12, 11	Высшее техническое	5	3
40	Кладовщик	14/39	Кладовщик/13	39	Высшее военное	3	1

Структура защищаемой информации

№ п\п	Наименование источника информации	Гриф	Источник информации	Место нахождения источника информации
1	Структура предприятия	К	Контракты, документы на бумажных носителях, персонал	Сейф с документами, каб. 3; ПК 33, 32, 37
2	Личные сведения о сотрудниках	ПДн	Документы на бумажных и электронных носителях, БД, персонал	Сейф с документами, каб. 3; сейф в кассе, ПК 15, 16

Окончание

№ п\п	Наименование источника информации	Гриф	Источник информации	Место нахождения источника информации
3	Учредительные документы	К	Нормативно-регламентирующие бумажные документы	Рабочий стол в кабинете директора, сейф с документами, каб. 3; ПК 33, 37
4	База данных клиентов, партнеров	ДСП	Документы на бумажных и электронных носителях, гл. бухгалтер	Сейф с документами, каб. 3; ПК 33, 25, 36
5	Пароли к используемому ПО и web-сайтам	ДСП	Документы на электронных носителях, СБ, отдел IT	ПК 15, 41
6	Архив различных версий разрабатываемых ПО, web-сайтов	СК	Документы на электронных носителях, СБ, отдел IT	ПК 30, 41
7	Регистрационные БД клиентов	ДСП	Документы на бумажных и электронных носителях	Сейф с документами, каб. 3; ПК 32, 25, 36
8	Методы и способы производства, новые технологии	ДСП	Документы на бумажных и электронных носителях	Сейф с документами, каб. 3; ПК 33, 36
9	Планы по реорганизации и развитию деятельности организации	ДСП	Документы на бумажных и электронных носителях	Сейф с документами, каб. 3; ПК 33, 25, 37
10	Планы и характер рекламной и публикаторской деятельности	ДСП	Документы на бумажных и электронных носителях, юрисконсульты	Сейф с документами, каб. 3; ПК 36, 34
11	Кадровый состав и его формирование	СК	Документы на бумажных и электронных носителях, бухгалтерия, ОК, стол директора	Сейф с документами, каб. 3; ПК 25, 36, 35
12	Сведения о системе безопасности организации	ДСП	Документы на бумажных и электронных носителях, СБ, рабочий стол директора	Сейф с документами, каб. 3; ПК 15, 16
13	Телефонные переговоры сотрудников и клиентов	ДСП	Документы на электронных носителях, СБ, отдел IT	ПК 15
14	Направления модернизации известных технологий, процессов и оборудования	ДСП	Документы на бумажных и электронных носителях	Сейф с документами, каб. 3; ПК 33, 36

Вариант № 6

Объект – производственная организация в сфере энергетики (торговли и маркетинга, название придумать самостоятельно), занимающая (арендующая) 1-й этаж двухэтажного кирпичного здания без постов охраны. Охранно-пожарная сигнализация сводится в помещение 1-го этажа. В здании 2-й этаж, подвал и смежные помещения занимают (арендуют) прочие «не охраняемые» собственники.

Перекрытия полов и потолков капитальные, из железобетонных панелей. Все внутренние двери деревянные, филенчатые, полнотелые. Двери в служебные кабинеты и бухгалтерию, кассу, архив, серверную и другие имеют по одному врезному замку. Двери в холлах, коридорах, тамбурах остекленные в верхней половине двери и запорных устройств не имеют. Все внутренние перегородки и стены (кроме наружных по периметру здания) гипсокартонные, каркасные или в кирпич (полкирпича), не капитальные. Во всех служебных кабинетах имеются персональные компьютеры, на складе – дорогостоящие материальные ценности. В помещениях 10 и кассы установлены сейфы массой 150 – 200 кг без крепления к полу и стенам. Кабинет 10 – режимное помещение с хранением информации, составляющей коммерческую тайну.

Двери:

Д1 – дверь пластиковая, полнотелая, с одним врезным замком

Д2 – дверь цельнометаллическая, с одним врезным замком

Д3 – дверь пластиковая, с одним врезным замком, верхняя половина двери остеклена

Д4 – дверь пластиковая, с двумя врезными замками на расстоянии более 300 мм, верхняя половина двери остеклена

Д5 – ворота цельнометаллические, с двумя врезными замками, закрываются с внутренней стороны на два крюка

Окна:

О1 – окно пластиковое, с двойным остеклением, без защитных пленок, решетки отсутствуют

О2 – окно пластиковое, с двойным остеклением, без защитных пленок, решетка со стороны помещения из прутка D = 16 мм, размер ячейки 120×150 мм

О3 – окно пластиковое, с двойным остеклением, без защитных пленок, решетка со стороны помещения из прутка D = 12 мм, размер ячейки 200×200 мм

О4 – окно пластиковое, с двойным остеклением, без защитных пленок, решетка со стороны помещения из прутка D = 16 мм, размер ячейки 120×150 мм

Экспликация помещений объекта:

1 – 3 – служебные кабинеты; 4 – служебный кабинет; 5 – склад; 6 – служебный кабинет; 7 – служебный кабинет; 8 – служебный кабинет; 9 – серверная; 10 – канцелярия; 11 – фойе; 12 – 14 – служебные кабинеты; 15 – бухгалтерия с кассой; 16 – 17 – служебные кабинеты; 18 – коридор; 19 – гараж; 20 – архив; 21 – служебный кабинет.

Структура организации:

Во главе стоит генеральный директор (каб. 12).

В штате организации:

– канцелярия (каб. 8), в штате: зав. канцелярией и два секретаря (один – в каб. 8 и один – в приемной (пом. 12)), зав. архивом (пом. 20);

– служба безопасности (пом. 16 – 17), в штате: начальник СБ (каб. 16) и подразделения (группа охраны и режима – ст. инспектор и инспектор (каб. 16); группа режима КТ – один инспектор (каб. 17); группа ИБ и ТЗИ – один администратор безопасности (каб. 10), ст. инспектор и инспектор (каб. 17), ст. юрисконсульт по безопасности (каб. 7);

– бухгалтерия с кассой (каб. 15), в штате: гл. бухгалтер (каб. 15), экономист, два бухгалтера, кассир;

– финансово-экономический отдел (каб. 21), в штате: начальник отдела, ст. экономист, экономист, инженер 1-й категории;

– отдел маркетинга (каб. 14), в штате: начальник отдела, ст. маркетолог-аналитик, два маркетолога-аналитика, бренд-менеджер; менеджер по торговым маркам и продуктам (все занимают каб. 14);

– отдел по работе с клиентами (каб. 13), в штате: начальник отдела (каб. 13), гл. специалист, ст. специалист, инженер 1-й категории;

– служба автоматизации (IT) (каб. 10), в штате: системный администратор и два инженера технической поддержки 1-й категории;

– служба главного энергетика (каб. 1 – 3), в штате: гл. энергетик, зам. гл. энергетика, ведущий инженер (все занимают каб. 1); два инженера 1-й категории (каб. 3); группа по ОТ и ТБ (каб. 2) – ст. инженер по ОТ и ТБ, инженер по ТБ и пожарной безопасности;

– техническая служба (каб. 4, 6), в штате: начальник службы, два ведущих специалиста (каб. 4), два инженера-проектировщика и два инженера 1-й категории (каб. 6);

– отдел кадров и договорно-правовой работы (каб. 7), в штате: начальник отдела, ст. инспектор ОК, юрисконсульт по договорно-правовой работе.

Технической службе подчиняется кладовщик (каб. 5).

Отделу кадров подчиняются: зав. гаражом, три водителя, слесарь-сантехник – 0,5 ставки, электрик – 0,5 ставки, дворник – 0,5 ставки, уборщицы – 1,0 ставки.

В структуре СБ основные задачи структурных подразделений следующие:

– группа охраны и режима: контроль обеспечения охраны объекта со стороны частной охранной организации, контроль работоспособности ОТС, СКУД и СВН, контроль эксплуатационно-технического обслуживания данных систем, обеспечение КПиОР, доставка ценных грузов, проверка почтовых сообщений;

– группа режима КИ – контроль ведения конфиденциального делопроизводства, работа с персоналом и посетителями, контроль публикаторской и издательской деятельности, работа со СМИ, контроль обеспечения режима КТ;

– группа ИБ и ТЗИ: администрирование безопасности ЛВС и ЭВМ, защищенные технологии обработки информации, техническая защита от утечки информации по техническим каналам;

– юрисконсульт по безопасности: юридическое сопровождение обеспечения безопасности, организационное обеспечение ИБ, аналитическая работа.

Штатный персонал объекта: общая характеристика (кроме обслуживающего персонала, основных и вспомогательных рабочих)

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
1	Руководство	12/2	Ген. директор/12	2, 1	Высшее техническое	7	6
2	Канцелярия	8/21	Зав. канцелярией/4	21, 22, 1, 47	Высшее техническое	5	5
3	Канцелярия	8/22	Секретарь/6	22, 1	Среднее специальное	4	4
4	Канцелярия	12/1	Секретарь/7	1, 22	Высшее гуманитарное	4	4
5	Канцелярия	20/47	Зав. архивом/15	47, 22	Высшее гуманитарное	5	5
6	Служба безопасности	16/48	Начальник СБ/8	48, 49, 50, 51, 27, 52, 53, 20	Высшее военное	8	6
7	Служба безопасности	16/49	Ст. инспектор СБ/5	49, 50	Высшее техническое	7	6
8	Служба безопасности	16/50	Инспектор СБ/6	50, 49	Высшее гуманитарное	8	7
9	Служба безопасности	17/51	Инспектор группы режима КТ/4	51, 21, 22, 1, 47	Высшее гуманитарное	6	6
10	Служба безопасности	10/27 (9/23)	Администратор безопасности/3	Все (1 – 53)	Высшее техническое профильное	10	9
11	Служба безопасности	17/52	Ст. инспектор СБ (ИБ и ТЗИ)/6	52, 53	Высшее техническое профильное	8	8

Продолжение

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
12	Служба безопасности	17/53	Инспектор СБ (ИБ и ТЗИ)/7	53, 52	Высшее гуманитарное	6	6
13	Служба безопасности	7/20	Ст. юрисконсульт/6	20	Высшее военное	5	5
14	Бухгалтерия	15/39	Гл. бухгалтер/13	39, 40, 41, 42, 38	Высшее экономическое	5	5
15	Бухгалтерия	15/40	Экономист/14	40, 41, 42, 38	Высшее экономическое	4	4
16	Бухгалтерия	15/41	Бухгалтер/15	41, 42, 38	Высшее экономическое	3	2
17	Бухгалтерия	15/42	Бухгалтер/9	42, 41	Среднее специальное	3	2
18	Бухгалтерия	Касса/38	Кассир/4	38	Среднее специальное	2	2
19	Финансово-экономический отдел	21/43	Начальник ФЭ отдела/16	43, 44, 45, 46,	Высшее экономическое	4	4
20	Финансово-экономический отдел	21/44	Ст. экономист/6	44, 45	Высшее экономическое	5	4
21	Финансово-экономический отдел	21/45	Экономист/14	45, 44, 46	Высшее экономическое	6	6
22	Финансово-экономический отдел	21/46	Инженер 1-й категории/13	46	Высшее гуманитарное	4	3
23	Отдел маркетинга	14/32	Начальник отдела маркетинга/9	32, 33, 34, 35, 36, 37	Высшее экономическое	5	4

Продолжение

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
24	Отдел маркетинга	14/33	Ст. маркетолог-аналитик/6	33, 34, 35	Среднее специальное	7	6
25	Отдел маркетинга	14/34	Маркетолог-аналитик/5	34, 35	Высшее экономическое	5	5
26	Отдел маркетинга	14/35	Маркетолог-аналитик/9	35, 34	Среднее специальное	4	4
27	Отдел маркетинга	14/36	Бренд-менеджер/4	36, 37	Среднее специальное	5	5
28	Отдел маркетинга	14/37	Менеджер по торговым маркам и продуктам/3	37, 36	Высшее экономическое	4	4
29	Отдел по работе с клиентами	13/28	Начальник отдела/15	28, 29, 30, 31	Высшее техническое	6	5
30	Отдел по работе с клиентами	13/29	Гл. специалист/13	29, 30	Высшее техническое	7	5
31	Отдел по работе с клиентами	13/30	Ст. специалист/17	30, 29	Высшее техническое профильное	5	5
32	Отдел по работе с клиентами	13/31	Инженер 1-й категории/13	31, 30	Высшее техническое	6	5
33	Служба автоматизации (IT)	10/24 (9/23)	Системный администратор/8	Все (1 – 53)	Высшее техническое	8	8

Продолжение

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
34	Служба автоматизации (IT)	10/25	Инженер технической поддержки 1-й категории/12	Все (1 – 53)	Высшее техническое профильное	7	7
35	Служба автоматизации (IT)	10/26	Инженер технической поддержки 1-й категории/12	Все (1 – 53)	Высшее экономическое	7	7
36	Служба главного энергетика	1/13	Гл. энергетик/4	13, 14, 15, 16, 17, 11, 12	Высшее техническое профильное	6	6
37	Служба главного энергетика	1/14	Зам. гл. энергетика/7	14, 15, 16	Высшее техническое	5	3
38	Служба главного энергетика	1/15	Ведущий инженер/5	15, 14	Высшее техническое	6	4
39	Служба главного энергетика	3/16	Инженер 1-й категории/12	16, 17	Высшее техническое профильное	4	3
40	Служба главного энергетика	3/17	Инженер 1-й категории/16	17, 16	Высшее техническое	3	2
41	Группа по ОТ и ТБ	2/11	Ст. инженер по ОТ и ТБ/3	11, 12	Высшее техническое	5	3
42	Группа по ОТ и ТБ	2/12	Инженер по ТБ и пожарной безопасности/7	12, 11	Высшее техническое	4	3

Окончание

№ п/п	Структурное подразделение	Расположение (номер кабинета/ номер ПК)	Должность/ стаж работы в должности, лет	Имеет доступ на ПК (номера ПК)	Образование	Уровень пользования ПК (градация от 1 до 10)	Знания и навыки в области ИБ (градация от 1 до 10)
43	Отдел кадров	7/18	Начальник отдела/12	18, 19	Высшее техническое	3	3
44	Отдел кадров и ДП работы	7/18	Ст. инспектор ОК/4	18, 19	Высшее техническое	2	1
45	Отдел кадров и ДП работы	7/19	Юрисконсульт по правовой работе/3	19, 18	Высшее экономическое	4	4
46	Техническая служба	4/8	Начальник службы/13	8, 9, 10, 3, 4, 5, 6, 7	Высшее техническое	5	4
47	Техническая служба	4/9	Ведущий специалист/4	9, 10	Высшее экономическое	4	4
48	Техническая служба	4/10	Ведущий специалист/6	10, 9	Высшее техническое	3	3
49	Техническая служба	6/3	Инженер-проектировщик/5	3, 4	Высшее техническое	5	4
50	Техническая служба	6/4	Инженер-проектировщик/3	4, 3	Высшее экономическое	6	4
51	Техническая служба	6/5	Инженер 1-й категории/4	5, 6	Высшее техническое	5	5
52	Техническая служба	6/6	Инженер 1-й категории/6	6, 5	Высшее техническое	6	4
53	Кладовщик	5/7	Кладовщик/4	7, 5	Среднее специальное	3	2

Структура защищаемой информации

№ п\п	Наименование источника информации	Гриф	Источник информации	Место нахождения источника информации
1	Структура предприятия	К	Контракты, документы на бумажных носителях, персонал организации	Сейф с документами, каб. 10; ПК 1, 2, 48
2	Личные сведения о сотрудниках фирмы	ПДн	Документы на бумажных и электронных носителях, БД, персонал организации	Сейф с документами, каб. 10; ПК 24, 25
3	Учредительные документы	К	Устав организации, бумажные документы	Рабочий стол в кабинете директора, секретаря; ПК 1, 2, 39, 32
4	Сведения о кредитах, контрактах	К	Документы на бумажных и электронных носителях, БД, гл. бухгалтер	Сейф с документами, каб. 10; ПК 1, 2, 39, 32, 19
5	База данных заказчиков, партнеров фирмы	КТ	Документы на бумажных и электронных носителях, гл. бухгалтер	Сейф с документами, каб. 10; ПК 19, 32, 39
6	Сведения о конкурентах (в том числе компромат)	КТ	Документы на бумажных и электронных носителях	Сейф с документами, каб. 10; ПК 32, 2
7	Сведения о распределении прибыли между сотрудниками	К	Документы на бумажных и электронных носителях, гл. бухгалтер	Сейф с документами, каб. 10; ПК 2, 39
8	Список отсутствующих сотрудников, сроки их отсутствия	СК	Документы на бумажных и электронных носителях, бухгалтерия, ОК	Сейф с документами, каб. 10; ПК 24; 25
9	Пароли к используемому ПО и web-сайтам	КТ	Документы на электронных носителях, СБ, отдел IT	ПК 24, 27
10	Архив различных версий разрабатываемых ПО, web-сайтов	СК	Документы на электронных носителях, СБ, отдел IT	ПК 24, 27
11	Архив названий, логотипов, рекламных буклетов и роликов фирм-заказчиков	СК	Документы на бумажных и электронных носителях, отдел маркетинга	Сейф с документами, каб. 10; ПК 24, 19, 20, 32

Окончание

№ п\п	Наименование источника информации	Гриф	Источник информации	Место нахождения источника информации
12	Сведения о концепте и продвижении продукции	КТ	Документы на бумажных и электронных носителях, отдел маркетинга	Сейф с документами, каб. 10; ПК 2, 32
13	Методы и способы производства, новые технологии	КТ	Документы на бумажных и электронных носителях, отдел маркетинга	Сейф с документами, каб. 10; ПК 2, 32
14	Конкурентоспособность производимой продукции, эффективность экспорта и импорта, предполагаемое время выхода на рынок	СК	Документы на бумажных и электронных носителях, отдел маркетинга	Сейф с документами, каб. 10; ПК 24, 25
15	Планы и характер рекламной и публикаторской деятельности	КТ	Документы на бумажных и электронных носителях, юрисконсульты	Сейф с документами, каб. 10; ПК 19, 20
16	Кадровый состав и его формирование	СК	Документы на бумажных и электронных носителях, бухгалтерия, ОК, стол директора	Сейф с документами, каб. 10; ПК 24, 25
17	Сведения о системе безопасности организации	КТ	Документы на бумажных и электронных носителях, СБ, рабочий стол директора	Сейф с документами, каб. 10; ПК 1, 48
18	Телефонные переговоры сотрудников и клиентов	КТ	Документы на электронных носителях, СБ, отдел IT	ПК 1, 48, 27
19	Направления модернизации известных технологий, процессов и оборудования	КТ	Документы на бумажных и электронных носителях, отдел маркетинга	Сейф с документами, каб. 10; ПК 1, 32
20	Изобретения и полезные модели, используемые инновации и ноу-хау производства	КТ	Документы на бумажных и электронных носителях, отдел маркетинга	Сейф с документами, каб. 10; ПК 24, 25

ЗАКЛЮЧЕНИЕ

В ходе выполнения курсовой работы обучающиеся формируют навыки по проведению аудита информационной безопасности, которые позволяют:

– выявить значимые угрозы для информации, циркулирующей в структурных компонентах АИС предприятия;

– оценить вероятность каждого события в инфраструктуре АИС, представляющего угрозу для безопасности, и ущерб от него;

– составить неформальную модель нарушителя АИС предприятия;

– определить основные требования к системе защиты АИС на предприятии;

– оценить с точки зрения этих требований эффективность применяемых организационных мер и инженерно-технических средств защиты;

– разработать предложения и рекомендации по совершенствованию комплексной системы обеспечения безопасности АИС на предприятии.

Проведение аудита безопасности АИС предприятия с использованием специализированного бесплатного программного обеспечения Microsoft Security Assessment Tool дает возможность:

– обеспечить формирование единой политики и концепции безопасности информации в АИС предприятия;

– рассчитать, согласовать и обосновать необходимые затраты на защиту информации в АИС предприятия;

– объективно и независимо оценить текущий уровень информационной безопасности в АИС предприятия;

– эффективно создавать и использовать профили защиты конкретного АИС предприятия на основе неоднократно апробированных и адаптированных качественных и количественных методик оценки информационной безопасности АИС предприятий заказчика;

– объективно оценить безопасность всех основных компонентов и сервисов корпоративной информационной системы предприятия, техническое состояние аппаратно-программных средств защиты информации (межсетевые экраны, маршрутизаторы, хосты, серверы, корпоративные БД и приложения);

– успешно применять на практике рекомендации, полученные в ходе аналитического исследования, для нейтрализации и локализации выявленных уязвимостей аппаратно-программного уровня в АИС предприятия.

Аудит информационной безопасности АИС в современных условиях – один из наиболее эффективных инструментов получения независимой и объективной оценки текущего уровня защищенности информационных ресурсов. Применение аудита информационной безопасности в АИС на практике должно быть не эпизодическим, а регулярным, позволяющим не только выявлять уже свершившиеся факты, но и предвидеть потенциальные угрозы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Чекулаева, Е. Н.* Управление информационной безопасностью : учеб. пособие / Е. Н. Чекулаева, Е. С. Кубашева ; Поволж. гос. технол. ун-т. – Йошкар-Ола : Поволж. гос. технол. ун-т, 2020. – 156 с. – ISBN 978-5-8158-2165-1.

2. *Шилов, А. К.* Управление информационной безопасностью : учеб. пособие / А. К. Шилов ; Юж. федер. ун-т, Ин-т компьютер. технологий и информ. безопасности. – Ростов н/Д. ; Таганрог : Юж. федер. ун-т, 2018. – 121 с. – ISBN 978-5-9275-2742-7.

3. *Абденов, А.* Современные системы управления информационной безопасностью : учеб. пособие / А. Абденов, Г. Дронова, В. Трушин ; Новосиб. гос. техн. ун-т. – Новосибирск : Новосиб. гос. техн. ун-т, 2017. – 48 с. – ISBN 978-5-7782-3236-5.

4. *Веселов, Г. Е.* Менеджмент риска информационной безопасности : учеб. пособие / Г. Е. Веселов, Е. С. Абрамов, А. К. Шилов ; Юж. федер. ун-т, Инж.-технол. акад. – Таганрог : Юж. федер. ун-т, 2016. – 109 с. – ISBN 978-5-9275-2327-5.

5. *Аверченков, В. И.* Аудит информационной безопасности : учеб. пособие для вузов / В. И. Аверченков. – 3-е изд., стер. – М. : ФЛИНТА, 2016. – 269 с. – ISBN 978-5-9765-1256-6.

6. *Аверченков, В. И.* Служба защиты информации: организация и управление / В. И. Аверченков, М. Ю. Рытов. – 3-е изд., стер. – М. : ФЛИНТА, 2016. – 186 с. – ISBN 978-5-9765-1271-9.

7. *Жукова, М. Н.* Управление информационной безопасностью : учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. – Красноярск : Сиб. гос. аэрокосм. ун-т, 2012. – Ч. 2. – 100 с.

8. *Шаньгин, В. Ф.* Комплексная защита информации в корпоративных системах : учеб. пособие / В. Ф. Шаньгин. – М. : ФОРУМ : ИНФРА-М, 2022. – 592 с. – ISBN 978-5-8199-0730-6 (ФОРУМ).

9. *Щеглов, А. Ю.* Модели, методы и средства контроля доступа к ресурсам вычислительных систем : учеб. пособие / А. Ю. Щеглов. – СПб. : НИУ ИТМО, 2014. – 95 с.

10. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации [Электронный ресурс] : утв. 30 марта 1992 г. – URL: www.fstec.ru (дата обращения: 15.03.2023).

11. Методический документ. Методика оценки угроз безопасности информации [Электронный ресурс] : утв. 5 февр. 2021 г. – URL: www.fstec.ru (дата обращения: 15.03.2023).

12. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [Электронный ресурс] : приказ ФСТЭК России № 17 (2013 г.). – URL: www.fstec.ru (дата обращения: 15.03.2023).

13. О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 [Электронный ресурс] : приказ ФСТЭК России № 27 (2017 г.). – URL: www.fstec.ru (дата обращения: 15.03.2023).

14. *Торокин, А. А.* Инженерно-техническая защита информации : учеб. пособие / А. А. Торокин. – М. : Гелиос АРВ, 2005. – 960 с.

15. ГОСТ Р 54471-2011. Информация, сохраняемая в электронном виде. Рекомендации по обеспечению достоверности и надежности. – М. : Стандартинформ, 2012. – 42 с.

16. Р 50.1.056-2005. Техническая защита информации. Основные термины и определения. – М. : Стандартинформ, 2006.

17. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – М. : Стандартинформ, 2007. – 12 с.

18. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. – М. : Стандартинформ, 2018. – 12 с.

19. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – М. : Стандартинформ, 2018. – 20 с.

20. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М. : Стандартинформ, 2008. – 31 с.

21. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. – М. : Стандартинформ, 2007. – 24 с.

22. Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации [Электронный ресурс]. – URL: www.norma_tiv.kontur.ru (дата обращения: 15.03.2023).

23. ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. – М. : Госстандарт России, 2003. – 9 с.

24. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. – М. : Стандартинформ, 2014. – 56 с.

25. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. – М. : Стандартинформ, 2014. – 336 с.

26. ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. – М. : Стандартинформ, 2014. – 274 с.

27. ГОСТ Р 51898-2002. Аспекты безопасности. Правила включения в стандарты. – М. : Стандартинформ, 2018. – 8 с.

28. ГОСТ Р ИСО 31000-2010. Менеджмент риска. Принципы и руководство. – М. : Стандартинформ, 2012. – 26 с.

Учебное издание

Комплексная защита объектов информатизации. Книга 35

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Учебное пособие к выполнению курсовой работы

Автор-составитель
ТЕЛЬНЫЙ Андрей Викторович

Редактор Т. В. Евстюничева
Технический редактор Ш. Ш. Амирсейидов
Корректор Н. В. Пустовойтова
Компьютерная верстка Е. А. Кузьминой, А. Н. Герасина
Выпускающий редактор А. А. Амирсейидова

Подписано в печать 07.11.23.
Формат 60×84/16. Усл. печ. л. 13,02. Тираж 30 экз.
Заказ
Издательство
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых.
600000, Владимир, ул. Горького, 87.