Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Удмуртский государственный университет»
Филиал ФГБОУ ВО «УдГУ» в г. Воткинске

А. П. Кузнецов

Сертификация информационных систем

Практикум

Ижевск
2025

УДК 004.9:006.063(075.8)
ББК 32.972я73-5
К891

Рекомендовано к изданию Педагогическим советом филиала «УдГУ» в г. Воткинске.

Рецензент: канд. техн. наук, доцент, ООО «МастерЛинк» А. В. Гурьянов.

Кузнецов А. П.

К891 Сертификация информационных систем : практикум / А. П. Кузнецов. – Ижевск : Удмуртский университет, 2025. – 1 Мб. – Текст : электронный.

Объект практикума: процесс сертификации информационных систем в организациях.

Цель практикума: формирование практических навыков подготовки и проведения сертификации информационных систем в соответствии с нормативными требованиями.

О чём практикум: о процедуре сертификации ИС, подготовке документации, оценке соответствия стандартам безопасности, требованиях регуляторов и выполнении практических заданий по сертификации в учебных и рабочих кейсах.

Минимальные системные требования:
Celeron 1600 Mhz; 128 Мб RAM; Windows XP/7/8 и выше, 8x DVD-ROM
разрешение экрана 1024×768 или выше; программа для просмотра pdf.

Кузнецов Андрей Павлович
Сертификация информационных систем

Практикум

Подписано к использованию 30.12.2025
Объем электронного издания 1Мб
Издательский центр «Удмуртский университет»
426034, г. Ижевск, ул. Ломоносова, д. 4Б, каб. 021
Тел. : +7(3412)916-364 E-mail: editorial@udsu.ru

ОГЛАВЛЕНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В практикуме используются следующие термины с соответствующими определениями:

Информационная система (ИС) – совокупность информации, информационных технологий и средств обработки информации, обеспечивающих реализацию определённых функций.

Сертификация информационных систем – процедура подтверждения соответствия информационной системы установленным требованиям, нормативным документам и стандартам в области безопасности информации.

Информационная безопасность (ИБ) – состояние защищённости информации, при котором обеспечены её конфиденциальность, целостность и доступность.

Аттестация ИС – процедура оценки соответствия информационной системы требованиям безопасности информации в установленной области применения.

Угроза безопасности информации – потенциальное событие или действие, которое может привести к нарушению конфиденциальности, целостности или доступности информации.

Уязвимость – недостаток в системе, который может быть использован для реализации угрозы.

Риск информационной безопасности – вероятность наступления события, которое может привести к ущербу в результате реализации угрозы при наличии уязвимости.

Политика информационной безопасности – совокупность правил и процедур, направленных на защиту информации и управление рисками ИБ в организации.

Процесс сертификации – последовательность действий, включающая анализ системы, подготовку документации, проведение испытаний и аудит для подтверждения соответствия ИС установленным требованиям.

Нормативно-правовая база (НПБ) – совокупность законов, стандартов и приказов, регулирующих процессы защиты информации и сертификации ИС.

Конфиденциальность – свойство информации, заключающееся в том, что доступ к ней разрешён только определённому кругу лиц.

Целостность – свойство информации, при котором исключается её несанкционированное или случайное изменение.

Доступность – свойство информации, при котором обеспечивается возможность доступа к ней уполномоченных пользователей в требуемое время.

Заявитель – юридическое лицо или индивидуальный предприниматель, подавший заявку на проведение сертификации объекта.

Аудит информационной безопасности – независимая оценка процессов и средств защиты информации на соответствие установленным требованиям.

Испытания в целях сертификации – мероприятия, направленные на проверку соответствия характеристик ИС требованиям стандартов и нормативных документов.

Управление доступом – процесс предоставления, изменения и удаления прав доступа пользователей к информационным ресурсам.

Инцидент информационной безопасности – событие, которое приводит или может привести к нарушению политики информационной безопасности.

Система управления информационной безопасностью (СУИБ) – часть системы управления организации, основанная на подходе к рискам и предназначенная для создания, внедрения, мониторинга, анализа и совершенствования информационной безопасности.

ГОСТ – государственный стандарт, устанавливающий обязательные или рекомендуемые требования к объектам стандартизации.

ISO/IEC 27001 – международный стандарт, устанавливающий требования к системам менеджмента информационной безопасности.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

В практикуме применяют следующие сокращения и обозначения:

ИС – информационная система

ИБ – информационная безопасность

НПБ – нормативно-правовая база

ФЗ – Федеральный закон

ГОСТ – Государственный стандарт

СУИБ – система управления информационной безопасностью

СЭД – система электронного документооборота

ФСТЭК – Федеральная служба по техническому и экспортному контролю

ФСБ – Федеральная служба безопасности

ISO/IEC – Международная организация по стандартизации / Международная электротехническая комиссия

PCI DSS – Стандарт безопасности данных индустрии платёжных карт

IDS – система обнаружения вторжений

СУБД – система управления базами данных

ВВЕДЕНИЕ

В условиях активного развития информационных технологий и цифровой трансформации экономики вопросы обеспечения безопасности и надежности информационных систем (ИС) выходят на первый план. Сертификация информационных систем становится обязательным и необходимым этапом жизненного цикла ИС, обеспечивая их соответствие требованиям законодательства, отраслевых стандартов и нормативных документов по защите информации.

Настоящий практикум разработан для студентов специальности 09.02.07 «Информационные системы и программирование» и является прикладным инструментом для освоения дисциплины «Сертификация информационных систем». Он ориентирован на практическое применение знаний в области нормативно-правовой базы, процедур оценки соответствия, подготовки и анализа сертификационной документации, что необходимо для будущей профессиональной деятельности специалистов в сфере информационных технологий.

В методическом пособии представлены практические задания, охватывающие ключевые этапы и аспекты процесса сертификации ИС:

- анализ информационных систем и определение угроз их безопасности;
- исследование типов сертификации и сфер их применения;
- изучение деятельности участников процесса сертификации;
- анализ нормативных документов и их применения;
- разработка базовой политики информационной безопасности;
- анализ соответствия ИС требованиям нормативной базы;
- классификация объектов сертификации в рамках ИС;
- построение матрицы соответствия требованиям и объектам сертификации;
- подготовка плана сертификации и комплекта заявочной документации;
- анализ протоколов испытаний и заключений аудита;
- разработка плана устранения несоответствий, выявленных в ходе аудита;
- составление чек-листов и планов управления рисками;
- проведение оценки рисков и разработка мер их снижения.

Каждое задание практикума сопровождается чётко сформулированной целью, подробным описанием шагов выполнения и рекомендациями по оформлению отчётности. В заданиях используются кейсы и примеры, приближенные к реальной практике, что позволяет студентам приобрести опыт работы с типовыми ситуациями, возникающими в процессе сертификации ИС в организациях различного профиля.

Практикум будет полезен:

- студентам колледжей и техникумов ИТ-направлений для формирования прикладных компетенций в области сертификации ИС;
- преподавателям для организации практических занятий и проведения текущего контроля знаний;
- начинающим специалистам и стажёрам в сфере информационной безопасности, которые готовятся к выполнению сертификационных процедур в профессиональной деятельности;
- всем, кто стремится понять процессы сертификации и построения системы информационной безопасности с учётом требований регуляторов.

Использование данного практикума позволит студентам систематизировать и углубить свои знания в области сертификации ИС, а также подготовиться к реальным задачам, связанным с обеспечением безопасности и соответствия информационных систем требованиям законодательства и стандартов Российской Федерации.

ЗАДАНИЕ 1: АНАЛИЗ ИНФОРМАЦИОННОЙ СИСТЕМЫ И ОПРЕДЕЛЕНИЕ УГРОЗ

Цель: закрепить понимание основных компонентов информационной системы, принципов информационной безопасности и типов угроз.

Описание:

1. Выбор информационной системы: выберите любую информационную систему (реальную или вымышленную), с которой вы знакомы или которая вас интересует. Это может быть, например, банковская система, социальная сеть, система управления университетом, интернет-магазин или другое.

2. Анализ компонентов: опишите основные компоненты выбранной ИС, включая:

– Аппаратное обеспечение (примеры устройств и серверов).

– Программное обеспечение (примеры операционных систем и приложений).

– Данные (примеры типов информации, которые обрабатываются или хранятся).

– Персонал (примеры должностей и ролей).

– Процедуры (примеры основных рабочих процессов).

3. Определение угроз: определите и опишите не менее пяти угроз, которые могут возникнуть для выбранной ИС. Для каждой угрозы укажите:

– Тип угрозы (например, вирус, хакерская атака, ошибка персонала).

– Вероятность возникновения (низкая, средняя, высокая).

– Возможные последствия (какой ущерб может быть нанесен ИС и ее пользователям).

– Меры, которые могут быть приняты для снижения риска.

4. Пример: для социальной сети одной из угроз может быть кража паролей пользователей. Это будет считаться хакерской атакой (тип угрозы), вероятность средняя (можно указать конкретную статистику), последствия – потеря данных, дискредитация ресурса, меры – регулярная смена паролей пользователями, использование двухфакторной аутентификации и другие.

Ресурсы:

– Материалы Лекции 1.

– Статьи по информационной безопасности (можно использовать поисковые системы, кибербезопасность на habr.com).

– Реальные примеры инцидентов информационной безопасности из новостей.

Форма представления: отчет в формате Word, включающий:

– Название выбранной ИС.

– Описание компонентов.

– Таблицу с описанием угроз и оценкой их последствий.

ЗАДАНИЕ 2: ИССЛЕДОВАНИЕ ТИПОВ СЕРТИФИКАЦИИ И СФЕР ИХ ПРИМЕНЕНИЯ

Цель: закрепить понимание типов сертификации ИС (обязательная, добровольная) и их применения в различных сферах.

Описание:

1. Выбор сферы: выберите одну из следующих сфер:

– Финансовая сфера.

– Здравоохранение.

– Телекоммуникации.

– Транспорт.

– Промышленность.

– Государственный сектор.

– Или любую другую, которая вас интересует (согласовать с преподавателем).

2. Исследование сертификации: проведите исследование о типах сертификации, которые применяются в выбранной сфере. Для этого:

– Определите, какие типы ИС используются в этой сфере (например, для банков – это системы обработки транзакций, для медицинских учреждений – это электронные медицинские карты).

– Выясните, является ли сертификация ИС в данной сфере обязательной или добровольной.

– Перечислите не менее трех стандартов (национальных или международных), по которым может проводиться сертификация.

– Для каждого из стандартов кратко опишите его основные требования и цели.

3. Примеры: для финансовой сферы: обязательная сертификация по требованиям ФСТЭК и ФСБ для систем обработки персональных данных, добровольная сертификация по стандарту ISO 27001. Требования стандартов PCI DSS для защиты платежных карт и т.д.

Ресурсы:

– Материалы Лекции №1.

– Нормативные документы (ссылки на сайты регуляторов – ФСТЭК, ФСБ, Минздрав, и др.).

– Стандарты в области информационной безопасности (ISO, ГОСТ).

– Поисковые системы и ресурсы по сертификации.

Форма представления: Презентация PowerPoint или Word, включающая:

– Название выбранной сферы.

– Типы ИС, используемые в сфере.

– Типы сертификации (обязательная, добровольная).

– Описание стандартов и их требований.

ЗАДАНИЕ 3: АНАЛИЗ УЧАСТНИКОВ ПРОЦЕССА СЕРТИФИКАЦИИ

Цель: закрепить понимание ролей и функций различных участников процесса сертификации (орган сертификации (ОС), испытательная лаборатория (ИЛ), заявитель, аудитор).

Описание:

1. Выбор участника: выберите одного из участников процесса сертификации (ОС, ИЛ, заявитель, аудитор).

2. Исследование деятельности: проведите исследование деятельности выбранного участника. Для этого найдите и изучите информацию о:

– Основные функции и обязанности выбранного участника.

– Требования к организации или специалистам, работающим в выбранной роли (например, аккредитация, наличие сертификатов, опыт работы).

– Примеры деятельности (например, для ОС – примеры проведения сертификации, для ИЛ – примеры проводимых испытаний, для аудитора – примеры аудиторских отчетов).

– Соблюдение норм этики и требований к независимости.

3. Анализ взаимодействия: опишите, как выбранный участник взаимодействует с другими участниками процесса сертификации.

4. Примеры: для органа по сертификации (ОС): пример аккредитованной компании, перечень проводимых работ. Для испытательной лаборатории (ИЛ): примеры проводимых испытаний (например, тестирование на проникновение).

Ресурсы:

– Материалы Лекции № 1.

– Сайты органов по сертификации, испытательных лабораторий (Рос аккредитация, ФСТЭК).

– Статьи о сертификации ИС и аудитах информационной безопасности.

– Сайты компаний, которые предоставляют услуги в области сертификации ИС.

Форма представления: отчет в формате Word, включающий:

– Название выбранного участника процесса сертификации.

– Описание функций и обязанностей выбранного участника.

– Требования к квалификации и аккредитации.

– Примеры деятельности выбранного участника.

– Описание взаимодействия с другими участниками процесса сертификации.

ЗАДАНИЕ 4: АНАЛИЗ НОРМАТИВНОГО ДОКУМЕНТА (НА ВЫБОР)

Цель: развить навыки работы с нормативной документацией, умение анализировать ее структуру и содержание, выделять ключевые положения и требования.

Описание:

1. Выберите один из предложенных нормативных документов:

– Федеральный закон "Об информации, информационных технологиях и о защите информации" (№ 149-ФЗ)

– Федеральный закон "О персональных данных" (№ 152-ФЗ)

– ГОСТ Р ИСО/МЭК 27001 "Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"

– ГОСТ Р ИСО/МЭК 27002 "Информационная технология. Методы обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности"

– Приказ ФСТЭК России №17 от 11.02.2013 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"

– Один из стандартов серии ГОСТ Р ИСО/МЭК 27030

2. Тщательно изучите выбранный документ. ознакомьтесь с его структурой, содержанием, ключевыми понятиями и требованиями.

3. Проведите анализ документа по следующим пунктам:

– Цель и область применения документа: для чего предназначен данный документ? Какие вопросы он регулирует? На кого распространяется его действие?

– Основные термины и определения: какие ключевые понятия используются в документе? Как они определяются?

– Основные положения и требования: какие основные правила, нормы или требования устанавливает документ? Какие обязательства возлагаются на субъекты, которых он регулирует?

– Структура документа: как организован документ? Какие разделы и подразделы он содержит?

– Связь с другими нормативными документами: как данный документ соотносится с другими нормативными документами в области информационной безопасности (например, с другими федеральными законами, стандартами или приказами регуляторов)?

– Примеры практического применения: где и как на практике применяются требования данного документа? Приведите примеры ситуаций, когда его положения становятся актуальными.

4. Оформите результаты анализа в письменном виде. Представьте отчет, включающий подробное описание результатов анализа по каждому из указанных пунктов. Отчет должен быть оформлен в деловом стиле, грамотно и четко.

ЗАДАНИЕ 5: РАЗРАБОТКА БАЗОВОЙ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель: применить теоретические знания на практике, разработать базовый документ, определяющий основные направления политики информационной безопасности организации.

Описание: представьте, что вы являетесь специалистом по информационной безопасности в некоторой вымышленной организации (например, в небольшой IT-компании, интернет-магазине или образовательном учреждении). Ваша задача – разработать проект базовой политики информационной безопасности для этой организации.

1. Определите контекст вашей организации:

– Опишите сферу деятельности вашей вымышленной организации, её основные бизнес-процессы и виды деятельности.

– Определите основные информационные активы организации (например, персональные данные клиентов, данные о продажах, интеллектуальная собственность).

– Опишите основные угрозы информационной безопасности, актуальные для вашей организации (например, утечка данных, несанкционированный доступ, вредоносное программное обеспечение).

2. Разработайте проект политики информационной безопасности. Проект должен включать следующие разделы:

– Цели и задачи политики информационной безопасности: каковы основные цели и задачи политики информационной безопасности вашей организации? Что она должна обеспечить?

– Область применения: на кого распространяется действие данной политики? На какие информационные системы и активы она распространяется?

– Основные принципы информационной безопасности: какие принципы лежат в основе политики информационной безопасности (например, конфиденциальность, целостность, доступность, подотчетность)?

– Роли и ответственность в области информационной безопасности: кто несет ответственность за обеспечение информационной безопасности в вашей организации? Какие обязанности у каждого из участников?

– Основные направления и меры обеспечения информационной безопасности: какие меры организационного и технического характера будут применяться для обеспечения информационной безопасности в вашей организации? (например, управление доступом, защита от вредоносного ПО, резервное копирование, обучение персонала, управление инцидентами и т.д.)

3. Используйте при разработке политики требования стандартов (ГОСТ Р ИСО/МЭК 27001, 27002 и т.д.) и законодательства РФ (ФЗ №149 и 152). Приведите конкретные примеры, как эти требования отражаются в вашей политике.

4. Оформите проект политики информационной безопасности в письменном виде. Представьте документ, оформленный в деловом стиле, четко и грамотно.

ЗАДАНИЕ 6: АНАЛИЗ СООТВЕТСТВИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ТРЕБОВАНИЯМ НОРМАТИВНОЙ БАЗЫ

Цель: применить полученные знания для анализа конкретной информационной системы на предмет ее соответствия требованиям нормативной базы.

Описание:

1. Выберите описание некоторой информационной системы. Это может быть:

– Описание существующей информационной системы организации.

– Описание информационной системы, представленное в виде кейса.

– Упрощенное описание вымышленной информационной системы.

– Описание реальной информационной системы, доступное в открытых источниках.

Описание должно включать:

– Назначение и функции системы.

– Типы обрабатываемой информации (включая, если есть, персональные данные).

– Основные компоненты системы (аппаратные, программные, сетевые).

– Меры защиты информации (если таковые имеются).

2. Проанализируйте выбранную информационную систему на предмет соответствия требованиям следующих нормативных документов:

– Федеральный закон "Об информации, информационных технологиях и о защите информации" (№ 149-ФЗ).

– Федеральный закон "О персональных данных" (№ 152-ФЗ) (если система обрабатывает персональные данные).

– ГОСТ Р ИСО/МЭК 27001 (в части общих требований к системе управления информационной безопасностью).

– Приказ ФСТЭК России №21 от 18.02.2013 (если система обрабатывает персональные данные).

– Другие применимые стандарты и нормативные документы (по согласованию с преподавателем).

3. Определите:

– Какие конкретные требования нормативных документов применимы к данной информационной системе.

– Насколько данная система соответствует или не соответствует этим требованиям.

– Какие недостатки и уязвимости существуют в системе с точки зрения информационной безопасности.

– Какие меры необходимо принять для приведения системы в соответствие с требованиями нормативной базы.

4. Представьте результаты анализа в письменном отчете. Отчет должен включать:

– Краткое описание анализируемой информационной системы.

– Перечень применимых нормативных документов.

– Результаты анализа по каждому нормативному документу (какие требования применимы, соответствие/несоответствие, недостатки и уязвимости).

– Рекомендации по устранению выявленных недостатков и приведению системы в соответствие требованиям.

ЗАДАНИЕ 7: КЛАССИФИКАЦИЯ ОБЪЕКТОВ СЕРТИФИКАЦИИ ДЛЯ ЗАДАННОГО ТИПА ИС

Цель: научиться определять и классифицировать потенциальные объекты сертификации в рамках заданного типа информационной системы, учитывая ее специфику и назначение.

Описание:

Вам предоставлено описание конкретного типа информационной системы. Ваша задача – определить и классифицировать все возможные объекты сертификации в рамках этой системы, разделив их на категории:

1. Тип информационной системы (выбрать один из списка):

– Система электронного документооборота (СЭД) в государственном учреждении.

– Интернет-магазин, обрабатывающий платежные данные клиентов.

– Облачный сервис хранения данных для частных лиц.

– Автоматизированная система управления технологическим процессом (АСУ ТП) на химическом предприятии.

– Информационная система управления персоналом (HRM) в крупной компании.

2. Для выбранного типа ИС определите следующие категории объектов сертификации:

– Аппаратное обеспечение: перечислите конкретные аппаратные компоненты, которые могут быть сертифицированы (например, серверы, сетевое оборудование, рабочие станции). Обоснуйте необходимость сертификации каждого компонента с точки зрения безопасности.

– Программное обеспечение: перечислите системное и прикладное программное обеспечение, которое может быть сертифицировано (например, операционные системы, СУБД, веб-серверы, специализированное ПО). Обоснуйте необходимость сертификации каждого элемента с точки зрения защиты информации.

– Сети и телекоммуникации: опишите, какие элементы сетевой инфраструктуры могут быть сертифицированы (например, брандмауэры, VPN-шлюзы, системы обнаружения вторжений). Обоснуйте необходимость сертификации каждого элемента для обеспечения безопасности передачи данных.

– Данные и базы данных: укажите, какие данные и базы данных могут быть сертифицированы (например, персональные данные клиентов, финансовая информация, конфиденциальные документы). Обоснуйте необходимость сертификации с точки зрения защиты конфиденциальности, целостности и доступности данных.

– Персонал: опишите, какие категории персонала, участвующие в работе ИС, могут быть сертифицированы (например, администраторы безопасности, разработчики, операторы). Обоснуйте необходимость сертификации с точки зрения повышения уровня знаний и навыков в области информационной безопасности.

– Процессы: опишите, какие процессы обработки информации, управления доступом, резервного копирования и восстановления могут быть сертифицированы. Обоснуйте необходимость сертификации для обеспечения безопасности и непрерывности бизнес-процессов.

– Услуги: опишите, какие услуги, предоставляемые ИС, могут быть сертифицированы (например, электронная почта, облачное хранение данных, веб-хостинг). Обоснуйте необходимость сертификации с точки зрения обеспечения безопасности и надежности предоставляемых услуг.

3. Представьте результаты в виде таблицы или списка, четко структурировав информацию по категориям и предоставив обоснование для каждого объекта сертификации.

ЗАДАНИЕ 8: РАЗРАБОТКА МАТРИЦЫ СООТВЕТСТВИЯ НОРМАТИВНЫМ ТРЕБОВАНИЯМ И ОБЪЕКТАМ СЕРТИФИКАЦИИ

Цель: научиться связывать требования нормативной базы с конкретными объектами сертификации в информационной системе, создавая матрицу соответствия для обеспечения более эффективной подготовки к сертификации.

Описание:

1. Выберите конкретную информационную систему. Это может быть система, описание которой вы использовали в Задании 1, или любая другая система.

2. Определите нормативную базу, применимую к выбранной ИС. Включите в список Федеральные законы (например, ФЗ-149, ФЗ-152), стандарты (например, ГОСТ Р ИСО/МЭК 27001) и приказы регуляторов (например, приказы ФСТЭК России).

3. Разработайте матрицу соответствия. Матрица должна содержать следующие столбцы:

– Нормативный документ: полное название нормативного документа (например, ФЗ "О персональных данных").

– Пункт нормативного документа: конкретный пункт, статья или раздел нормативного документа, содержащий требование (например, статья 18 ФЗ-152).

– Требование: краткое описание требования, сформулированное в нормативном документе (например, "Обеспечение конфиденциальности персональных данных").

– Объект сертификации: конкретный объект (или объекты) ИС, к которому относится данное требование (например, база данных персональных данных, система управления доступом).

– Меры защиты: описание конкретных мер, реализуемых для выполнения данного требования (например, шифрование данных, разграничение прав доступа, аудит доступа к данным).

– Соответствие (Да/Нет): оценка соответствия объекта сертификации данному требованию (на основе анализа имеющихся данных).

4. Заполните матрицу соответствия для выбранной информационной системы и применимой нормативной базы.

5. Сделайте выводы о том, какие объекты сертификации наиболее критичны для обеспечения соответствия требованиям нормативной базы, и какие меры защиты необходимо усилить.

Пример фрагмента матрицы соответствия:

Нормативный документ	Пункт нормативного документа	Требование	Объект сертификации	Меры защиты	Соответствие (Да/Нет)
ФЗ "О персональных данных"	Статья 18	Обеспечение конфиденциальности ПДн	База данных клиентов	Шифрование данных, разграничение прав доступа	Да
ФЗ "О персональных данных"	Статья 19	Защита ПДн от неправомерного доступа	Система управления доступом	Аутентификация, авторизация, аудит доступа	Нет
ГОСТ Р ИСО/МЭК 27001	7.2	Управление документацией	Политика ИБ	Регулярное обновление, утверждение руководством	Да

6. Представьте документ, оформленный в деловом стиле, четко и грамотно.

ЗАДАНИЕ 9: РАЗРАБОТКА ПЛАНА СЕРТИФИКАЦИИ ДЛЯ ВЫБРАННОГО ОБЪЕКТА ИС

Цель: научиться разрабатывать план сертификации для конкретного объекта информационной системы, учитывая его специфику, применимую нормативную базу и выбранные стандарты.

Описание:

1. Выберите конкретный объект сертификации. Это может быть один из объектов, определенных вами в предыдущих заданиях, или любой другой объект. Пример: «Система управления базами данных (СУБД) Oracle, используемая для хранения персональных данных клиентов интернет-магазина».

2. Определите цели сертификации: четко сформулируйте цели, которые должны быть достигнуты в результате сертификации (например, подтверждение соответствия требованиям ФЗ-152, повышение доверия клиентов, получение конкурентного преимущества).

3. Определите применимую нормативную базу и стандарты: укажите конкретные Федеральные законы, стандарты (например, ГОСТ Р ИСО/МЭК 27001, 27002) и приказы регуляторов, которые применимы к выбранному объекту сертификации.

4. Разработайте план сертификации. План должен включать следующие этапы:

– Подготовка: определение объема работ, формирование команды, разработка необходимых документов (например, политики безопасности, процедуры, руководства).

– Анализ соответствия: проведение анализа соответствия объекта сертификации требованиям нормативной базы и стандартов.

– Устранение несоответствий: разработка и реализация мер по устранению выявленных несоответствий.

– Выбор органа по сертификации: выбор аккредитованного органа по сертификации, имеющего опыт в сертификации объектов данного типа.

– Проведение сертификационного аудита: организация и проведение сертификационного аудита органом по сертификации.

– Получение сертификата: получение сертификата соответствия в случае успешного прохождения аудита.

– Поддержание сертификата: разработка плана мероприятий по поддержанию соответствия требованиям и регулярному обновлению сертификата.

5. Для каждого этапа плана определите:

– Задачи: конкретные задачи, которые необходимо выполнить на данном этапе.

– Ответственных: сотрудников или подразделения, ответственных за выполнение задач.

– Сроки: сроки выполнения каждого этапа.

– Ресурсы: необходимые ресурсы (например, финансовые, человеческие, технические).

6. Представьте план сертификации в виде диаграммы Ганта, четко структурировав информацию по этапам, задачам, ответственным, срокам и ресурсам.

ЗАДАНИЕ 10: ПОДГОТОВКА ЗАЯВКИ НА СЕРТИФИКАЦИЮ ДЛЯ ЗАДАННОЙ ИС

Цель: научиться правильно заполнять заявку на сертификацию, определять необходимый комплект документов и выбирать подходящий орган по сертификации.

Описание: ваша задача – подготовить полный комплект документов для подачи заявки на сертификацию этой ИС.

1. Выберите тип ИС:

– Веб-приложение для онлайн-банкинга.

– Система электронного документооборота (СЭД) в коммерческой организации.

– Медицинская информационная система (МИС) в частной клинике.

– Система видеонаблюдения в торговом центре.

– Система управления промышленным предприятием (MES).

2. Изучите описание выбранной ИС и определите:

– Полное наименование и реквизиты организации-заявителя (придумайте их).

– Полное наименование и описание объекта сертификации (максимально конкретно).

– Заявляемые требования (выберите применимые Федеральные законы, стандарты, приказы регуляторов - обоснуйте свой выбор).

– Информацию о производителе (разработчике) объекта сертификации (придумайте ее).

– Контактные данные лица, ответственного за проведение сертификации (придумайте их).

3. Подготовьте заявку на сертификацию:

– Заполните форму заявки (форма должна содержать все необходимые сведения, перечисленные в лекции).

– Подпишите заявку руководителем организации (или уполномоченным лицом) и заверьте печатью (придумайте ФИО и должность руководителя).

4. Составьте перечень документов, прилагаемых к заявке:

– Укажите все необходимые документы, которые должны быть приложены к заявке (техническое описание, руководство по эксплуатации, политика информационной безопасности, модель угроз и нарушителя, и т.д.).

– Обоснуйте необходимость включения каждого документа в перечень.

5. Выберите подходящий орган по сертификации (ОС):

– Изучите информацию о различных ОС (используйте интернет, профессиональные ресурсы).

– Выберите ОС, который соответствует требованиям (аккредитация, опыт, репутация, сроки, стоимость).

– Обоснуйте свой выбор ОС.

6. Представьте документы, оформленные в деловом стиле, четко и грамотно.

ЗАДАНИЕ 11: АНАЛИЗ ПРОТОКОЛА ИСПЫТАНИЙ И ЗАКЛЮЧЕНИЯ АУДИТА

Цель: научиться анализировать протоколы испытаний и заключения аудита, выявлять несоответствия и оценивать влияние выявленных несоответствий на безопасность ИС.

Описание: вам будет предоставлен протокол испытаний и заключение аудита для некоторой информационной системы (или для отдельных ее компонентов). Ваша задача – проанализировать эти документы и сделать выводы о соответствии ИС заявленным требованиям.

1. Получите от преподавателя протокол испытаний и заключение аудита. **Смотрите приложения к заданию.**
2. Внимательно изучите представленные документы и определите:

– Наименование объекта сертификации, для которого проводились испытания и аудит.

– Перечень нормативных документов, соответствие которым проверялось в ходе испытаний и аудита.

– Результаты испытаний: перечислите выявленные несоответствия (если есть) и дайте им оценку (критическое, значительное, незначительное).

– Результаты аудита: перечислите выявленные несоответствия (если есть) и дайте им оценку (критическое, значительное, незначительное).

– Выводы, содержащиеся в протоколе испытаний и заключении аудита.

3. Проведите собственный анализ результатов испытаний и аудита:

– Согласны ли вы с выводами, представленными в протоколе испытаний и заключении аудита? Обоснуйте свое мнение.

– Какие последствия для безопасности ИС могут иметь выявленные несоответствия?

– Какие меры необходимо предпринять для устранения выявленных несоответствий?

– Влияют ли выявленные несоответствия на возможность выдачи сертификата соответствия?

4. Сформулируйте общее заключение о соответствии ИС заявленным требованиям.

ПРИЛОЖЕНИЯ

Найти реальные протоколы испытаний и заключения аудита в открытом доступе практически невозможно. Это связано с тем, что эти документы содержат конфиденциальную информацию об информационной системе, ее уязвимостях и мерах защиты. Публикация такой информации может нанести серьезный ущерб безопасности организации.

Однако, для выполнения задания можно использовать примеры, которые имитируют реальные документы, но не содержат конфиденциальной информации. Ниже приведены примеры фрагментов протокола испытаний и заключения аудита, которые можно использовать в качестве основы для выполнения Задания.

Пример 1: Фрагмент протокола испытаний межсетевого экрана (Брандмауэра)

Протокол испытаний № 2023-10-001

Объект испытаний: Межсетевой экран (Брандмауэр) "SecureGate 2000" версии 2.5

Производитель: ООО "Защитные Системы"

Дата проведения испытаний: 2023-10-15

Испытательная лаборатория: ООО "Безопасность-Тест" (Аттестат аккредитации № АА-0001)

Перечень нормативных документов:

- ГОСТ Р 57580.1-2017 "Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Основные положения"
- ГОСТ Р 57580.2-2018 "Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия"
- Требования к межсетевым экранам, утвержденные ФСТЭК России (2016 г.)

Результаты испытаний:

№	Наименование теста	Результат	Оценка	Комментарии
1	Фильтрация трафика по IP-адресам и портам	Пройдено	-	Фильтрация работает корректно.
2	Обнаружение и блокировка DoS-атак	Пройдено	-	Брандмауэр эффективно обнаруживает и блокирует SYN flood, UDP flood и HTTP flood атаки.
3	Защита от SQL-инъекций	Не пройдено	Критично	Брандмауэр не блокирует попытки SQL-инъекций в веб-приложения. Необходимо включение соответствующего модуля защиты и его настройка.
4	Поддержка VPN-соединений (IPsec, L2TP)	Пройдено	-	VPN-соединения устанавливаются и функционируют корректно.
5	Журналирование событий безопасности	Пройдено	-	Журналирование работает корректно, в журнале фиксируются все значимые события безопасности.

Вывод:

Межсетевой экран "SecureGate 2000" в целом соответствует требованиям нормативных документов, за исключением пункта, касающегося защиты от SQL-инъекций. Для получения положительного заключения о соответствии необходимо включение и настройка модуля защиты от SQL-инъекций, а также проведение повторных испытаний.

Подпись:

Руководитель ИЛ ООО "Безопасность-Тест" _____ (ФИО)

Пример 2: Фрагмент заключения аудита информационной безопасности

Заключение аудита № АБ-2023-11-002

Объект аудита: Система электронного документооборота (СЭД) "OfficeFlow" версии 3.0

Организация: ООО "Деловые Решения"

Дата проведения аудита: 2023-11-05

Аудитор: ООО "ИнформАудит" (Лицензия ФСТЭК № ЛСЗ-0002)

Перечень нормативных документов:

- Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"
- ГОСТ Р ИСО/МЭК 27001-2011 "Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"

- Приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"

Результаты аудита:

№	Область аудита	Соответствие	Оценка	Комментарии
1	Политика информационной безопасности	Соответствует	-	Политика информационной безопасности разработана и утверждена, но требует актуализации в соответствии с изменениями в законодательстве.
2	Управление доступом	Частично	Значимо	Используются слабые пароли, отсутствует двухфакторная аутентификация. Требуется усиление мер защиты учетных записей.
3	Защита от вредоносного программного обеспечения	Соответствует	-	На рабочих станциях установлено антивирусное ПО, регулярно обновляются базы.
4	Резервное копирование и восстановление данных	Не соответствует	Критично	Процедура резервного копирования данных отсутствует. В случае сбоя или аварии данные могут быть потеряны. Требуется немедленная разработка и внедрение процедуры резервного копирования.
5	Физическая безопасность	Соответствует	-	Помещения, где размещено серверное оборудование, охраняются, доступ ограничен.

Вывод:

Система электронного документооборота "OfficeFlow" частично соответствует требованиям нормативных документов. Выявлены критичные и значимые несоответствия, требующие немедленного устранения. Для получения положительного заключения о соответствии необходимо:

- Разработать и внедрить процедуру резервного копирования данных.
- Усилить меры защиты учетных записей пользователей (использовать сложные пароли, внедрить двухфакторную аутентификацию).
- Актуализировать политику информационной безопасности.

Рекомендации:

1. Разработать план мероприятий по устранению выявленных несоответствий.

2. Провести повторный аудит после реализации плана мероприятий.

Подпись:

Аудитор ООО "ИнформАудит" _____ (ФИО)

Как использовать эти примеры для выполнения задания:

1. Изучите примеры внимательно: обратите внимание на структуру документов, перечень проверяемых требований, результаты и выводы.

2. Адаптируйте примеры к выбранному вами типу ИС: Измените наименование объекта сертификации, нормативные документы, результаты и выводы, чтобы они соответствовали вашей задаче.

3. Проведите собственный анализ: Не просто переписывайте информацию из примеров, а проведите собственный анализ результатов испытаний и аудита. Подумайте, какие последствия могут иметь выявленные несоответствия для безопасности ИС, и какие меры необходимо предпринять для их устранения.

Эти примеры помогут вам понять, как выглядят реальные протоколы испытаний и заключения аудита, и как их анализировать для оценки соответствия ИС заявленным требованиям.

Удачи в выполнении задания!

ЗАДАНИЕ 12: РАЗРАБОТКА ПЛАНА МЕРОПРИЯТИЙ ПО УСТРАНЕНИЮ НЕСООТВЕТСТВИЙ

Цель: научиться разрабатывать план мероприятий по устранению несоответствий, выявленных в ходе испытаний и аудита, а также оценивать эффективность этих мероприятий.

Описание: на основе анализа протокола испытаний и заключения аудита, выполненного в предыдущем Задании, разработайте план мероприятий по устранению выявленных несоответствий.

1. Используйте результаты анализа протокола испытаний и заключения аудита, выполненного в Задании 11.

2. Для каждого выявленного несоответствия разработайте план мероприятий по его устранению:

– Сформулируйте конкретные цели, которые необходимо достичь в результате реализации плана мероприятий (например, "Устранить уязвимость в веб-приложении, связанную с SQL-инъекциями").

– Определите перечень конкретных задач, которые необходимо выполнить для достижения поставленных целей (например, "Провести анализ кода веб-приложения", "Разработать и внедрить меры защиты от SQL-инъекций", "Провести повторное тестирование веб-при-ложения").

– Определите ответственных за выполнение каждой задачи (конкретные должности или подразделения).

– Определите сроки выполнения каждой задачи (конкретные даты или периоды времени).

– Определите необходимые ресурсы (финансовые, человеческие, технические).

3. Оцените эффективность разработанного плана мероприятий:

– Насколько вероятно, что предложенный план позволит устранить выявленные несоответствия?

– Какие риски связаны с реализацией плана (например, задержки, нехватка ресурсов, неэффективность предложенных мер)?

– Какие показатели можно использовать для оценки эффективности реализации плана (например, количество устраненных уязвимостей, процент соответствия требованиям безопасности)?

4. Представьте план мероприятий в виде диаграммы Ганта, четко структурировав информацию по несоответствиям, целям, задачам, ответственным, срокам и ресурсам.

Пример фрагмента плана мероприятий:

Несоответствие	Цель	Задачи	Ответственный	Сроки	Ресурсы
Отсутствие резервного копирования БД ПДн	Обеспечение возможности восстановления БД ПДн в случае сбоев	1. Разработка процедуры резервного копирования БД ПДн	Администратор БД	10.11.2023	5 часов рабочего времени, ПО для резервного копирования
		2. Настройка автоматического резервного копирования БД ПДн	Администратор БД	17.11.2023	3 часа рабочего времени, сервер для хранения резервных копий
		3. Тестирование процедуры восстановления из резервной копии	Администратор БД	24.11.2023	2 часа рабочего времени
Уязвимость SQL-инъекции в веб-приложении	Устранение возможности несанкционированного доступа к БД через веб-приложение	1. Проведение анализа кода веб-приложения на наличие SQL-инъекций	Разработчик ПО	15.11.2023	8 часов рабочего времени, инструмент для статического анализа кода
		2. Разработка и внедрение мер защиты от SQL-инъекций (экранирование, параметризованные запросы)	Разработчик ПО	22.11.2023	16 часов рабочего времени
		3. Проведение повторного тестирования веб-приложения на наличие SQL-инъекций	Тестировщик	29.11.2023	4 часа рабочего времени

ЗАДАНИЕ 13: РАЗРАБОТКА ЧЕК-ЛИСТА ДЛЯ АУДИТА ВЕБ-ПРИЛОЖЕНИЯ

Цель: научиться разрабатывать чек-листы, учитывающие специфику веб-приложения и охватывающие ключевые аспекты его безопасности.

Описание: представьте, что вы являетесь аудитором безопасности веб-приложения, которое обрабатывает персональные данные пользователей. Ваша задача – разработать чек-лист, который поможет вам провести комплексный аудит этого веб-приложения и оценить его соответствие требованиям безопасности.

1. Определите тип веб-приложения:
   – Интернет-магазин, обрабатывающий платежные данные.
   – Социальная сеть с личными профилями пользователей.
   – Система онлайн-банкинга.
   – Сервис электронной почты.
   – Система управления контентом (CMS) для корпоративного сайта.
2. Изучите применимые нормативные документы и стандарты:
   – Федеральный закон "О персональных данных" (ФЗ-152).
   – OWASP Top Ten.
   – ГОСТ Р ИСО/МЭК 27002-2021 "Информационная технология. Методы и средства обеспечения безопасности. Свод норм по управлению информационной безопасностью".
   – Отраслевые стандарты (например, PCI DSS для интернет-магазина).
3. Разработайте чек-лист, включающий следующие разделы:
   – Аутентификация и управление сессиями: например, «Используются ли сложные пароли?», «Реализована ли двухфакторная аутентификация?», «Как обрабатываются сессионные куки?».
   – Авторизация и управление доступом: например, «Разграничен ли доступ к данным в зависимости от ролей пользователей?», «Проверяются

ли права доступа перед выполнением операций?», «Проводится ли аудит действий пользователей?».

– Ввод и обработка данных: например, «Защищено ли веб-приложение от SQL-инъекций?», «Защищено ли веб-приложение от межсайтового скриптинга (XSS)?», «Проверяются ли введенные пользователем данные на соответствие формату?».

– Конфиденциальность данных: например, «Используется ли HTTPS для защиты трафика?», «Шифруются ли конфиденциальные данные при хранении?», «Удаляются ли конфиденциальные данные после окончания срока хранения?».

– Управление ошибками и журналирование: например, «Как обрабатываются ошибки в веб-приложении?», «Ведется ли журнал событий безопасности?», «Отслеживаются ли подозрительные события?».

– Конфигурация сервера и инфраструктуры: например, «Установлены ли последние обновления безопасности для сервера?», «Настроены ли брандмауэр и другие средства защиты?», «Ограничен ли доступ к административным интерфейсам?».

– Управление уязвимостями и обновления: например, «Как часто проводится сканирование уязвимостей?», «Как быстро устраняются выявленные уязвимости?», «Используются ли средства мониторинга безопасности?».

4. Для каждого пункта чек-листа укажите:

–Требование безопасности: четко сформулированное требование, которое необходимо проверить.

– Метод проверки: опишите метод, который вы будете использовать для проверки соответствия требованию (например, анализ исходного кода, тестирование, визуальный осмотр).

– Критерии оценки: укажите, какие критерии вы будете использовать для определения соответствия или несоответствия требованию.

– Поле для результата: «Соответствует», «Не соответствует», «Не применимо».

– Комментарии: поле для дополнительных замечаний и рекомендаций.

5. Оформите чек-лист в виде таблицы или списка.

Пример фрагмента чек-листа:

№	Требование	Метод проверки	Соответствует	Не соответствует	Не применимо	Комментарии
1	Наличие политики информационной безопасности	Анализ документации				
2	Разграничение доступа к информации в соответствии с должностными обязанностями	Анализ настроек прав доступа				
3	Использование сложных паролей	Интервью с персоналом				
4	Установка последних обновлений безопасности для операционной системы	Сканирование уязвимостей				
5	Наличие антивирусного программного обеспечения	Визуальный осмотр				
6	Регулярное резервное копирование данных	Анализ настроек резервного копирования				
...	...	...				...

№	Требование безопасности	Метод проверки	Критерии оценки	Результат	Комментарии
1	Все страницы, передающие конфиденциальную информацию (логин, пароль, данные кредитных карт), используют HTTPS	Анализ конфигурации веб-сервера	Проверка наличия SSL/TLS сертификата и корректности его настроек. Проверка использования HTTPS на страницах, где вводится или отображается конфиденциальная информация.		Проверить срок действия сертификата. Убедиться в использовании актуальных версий протоколов SSL/TLS и криптографических алгоритмов.
2	Веб-приложение защищено от SQL-инъекций	Тестирование, анализ кода	Отсутствие возможности выполнить произвольные SQL-запросы через пользовательский ввод. Использование параметризованных запросов или экранирования специальных символов.		Провести тестирование с использованием различных векторов атак. Проанализировать код на наличие уязвимых мест.

ЗАДАНИЕ 14: АНАЛИЗ ПОТЕНЦИАЛЬНЫХ УЯЗВИМОСТЕЙ ЗАДАННОГО КОМПОНЕНТА ИС

Цель: развить навыки анализа потенциальных уязвимостей, связанных с определенным типом компонентов информационной системы, и определения соответствующих мер защиты.

Описание: вместо практического использования сканера уязвимостей, в этом задании вам предлагается провести теоретический анализ потенциальных уязвимостей, которые могут быть присущи конкретному компоненту информационной системы.

1. Выберите компонент ИС:
   – Веб-сервер (например, Apache, Nginx).
   – Сервер базы данных (например, MySQL, PostgreSQL).
   – Операционная система (например, Windows Server, Linux).
   – Маршрутизатор или брандмауэр.
   – Система обнаружения вторжений (IDS).
2. Проведите исследование:
   – Изучите документацию по выбранному компоненту ИС.
   – Найдите информацию об известных уязвимостях, характерных для этого компонента.
   – Изучите рекомендации по обеспечению безопасности этого компонента.
3. Составьте отчет, включающий следующие разделы:
   – Краткое описание выбранного компонента ИС.
   – Перечень потенциальных уязвимостей, которые могут быть присущи этому компоненту.
   – Для каждой уязвимости укажите:
     - Наименование уязвимости.
     - Краткое описание уязвимости.
     - Потенциальные последствия эксплуатации уязвимости.

- Рекомендации по предотвращению или смягчению последствий эксплуатации уязвимости.

4. Структурируйте отчет в табличном виде.

Пример фрагмента отчета о потенциальных уязвимостях веб-сервера Apache:

Наименование уязвимости	**Описание**	**Потенциальные последствия**	**Рекомендации по предотвращению/ смягчению**
Разглашение информации через директории с включенным "Directory Listing"	Если в конфигурации Apache включена опция "Directory Listing" для определенных директорий, злоумышленник может получить список файлов и поддиректорий, что может привести к раскрытию конфиденциальной информации (например, исходного кода, резервных копий).	Раскрытие конфиденциальной информации. Возможность выявления дополнительных уязвимостей.	Отключите "Directory Listing" для директорий, содержащих конфиденциальную информацию. Настройте правила доступа, чтобы ограничить доступ к этим директориям только авторизованным пользователям.
Уязвимости, связанные с небезопасной конфигурацией SSL/TLS	Неправильная настройка SSL/TLS (например, использование устаревших протоколов, слабых шифров) может позволить злоумышленнику перехватить и расшифровать трафик, передаваемый между пользователем и сервером.	Перехват трафика. Раскрытие конфиденциальной информации (например, логинов, паролей, данных кредитных карт). Возможность осуществления атак "человек посередине".	Используйте актуальные версии протоколов TLS (1.2, 1.3). Отключите поддержку устаревших протоколов SSLv3, TLS 1.0, TLS 1.1. Используйте надежные шифры. Регулярно проверяйте конфигурацию SSL/TLS с помощью специализированных инструментов.
Уязвимости, связанные с использованием устаревших версий Apache	В устаревших версиях Apache могут присутствовать известные уязвимости, которые позволяют злоумышленнику выполнить произвольный код, получить несанкционированный доступ к данным или нарушить работу сервера.	Несанкционированное выполнение кода. Раскрытие конфиденциальной информации. Отказ в обслуживании (DoS).	Регулярно обновляйте Apache до последней стабильной версии. Отслеживайте информацию о новых уязвимостях и своевременно устанавливайте исправления безопасности.

ЗАДАНИЕ 15: ПРОВЕДЕНИЕ ИНТЕРВЬЮ С ПЕРСОНАЛОМ И АНАЛИЗ РЕЗУЛЬТАТОВ

Цель: научиться проводить интервью с персоналом для оценки уровня знаний и соблюдения правил безопасности, а также анализировать полученные результаты и делать выводы.

Описание: представьте, что вы проводите аудит безопасности в компании, где сотрудники активно используют информационные системы. Ваша задача – провести интервью с несколькими сотрудниками, оценить их уровень знаний в области информационной безопасности и составить отчет о результатах интервью.

1. Разработайте план интервью:

– Определите категории сотрудников, с которыми вы будете проводить интервью (например, рядовые сотрудники, администраторы, руководители).

– Разработайте список вопросов, охватывающих следующие темы:

- Знание политик и процедур безопасности компании.
- Соблюдение правил безопасности при работе с ИС.
- Осведомленность об угрозах безопасности.
- Реакция на инциденты безопасности.
- Уровень ответственности за обеспечение безопасности.

– Подготовьте вопросы, адаптированные для каждой категории сотрудников.

Примеры вопросов:

– «Знаете ли вы, где можно ознакомиться с политикой информационной безопасности компании?».

– «Какие требования предъявляются к сложности пароля в нашей компании?».

– «Как вы поступаете, если получили подозрительное письмо по электронной почте?».

– «Что вы делаете, если обнаружили вирус на своем компьютере?».

– «Кто несет ответственность за обеспечение безопасности информации в нашей компании?».

– «Как часто вы меняете свой пароль?».

– «Что такое фишинг, и как от него защититься?».

– «Что делать, если вы случайно отправили конфиденциальную информацию не тому адресату?».

2. Проведите интервью с 3-5 сотрудниками (можно провести смоделированное интервью с друзьями):

– Получите согласие на проведение интервью.

– Объясните цель интервью и гарантируйте конфиденциальность полученной информации.

– Задавайте вопросы из разработанного плана интервью.

– Внимательно слушайте ответы и делайте записи.

3. Проанализируйте результаты интервью:

– Оцените уровень знаний и соблюдения правил безопасности каждым сотрудником.

– Выявите общие тенденции и проблемы в компании.

– Определите области, требующие улучшения.

4. Составьте отчет о результатах интервью:

– Краткое описание цели и методики проведения интервью.

– Общие выводы о уровне знаний и соблюдения правил безопасности сотрудниками компании.

– Перечень выявленных проблем и недостатков.

– Рекомендации по улучшению ситуации (например, проведение обучения, пересмотр политик и процедур безопасности).

Пример фрагмента отчета о результатах интервью:

Сотрудник	Знание политик и процедур безопасности	Соблюдение правил безопасности	Осведомленность об угрозах безопасности	Реакция на инциденты безопасности	Выводы	Рекомендации
Иванов И.И.	Хорошо	Удовлетворительно	Удовлетворительно	Удовлетворительно	Знает основные положения политики безопасности, но не всегда соблюдает правила. Слабо осведомлен об угрозах безопасности.	Провести дополнительное обучение по основным правилам безопасности и видам угроз.
Петрова А.А.	Удовлетворительно	Хорошо	Хорошо	Хорошо	Знает правила безопасности и старается их соблюдать. Хорошо осведомлена об угрозах безопасности.	-
Сидоров С.С.	Плохо	Плохо	Плохо	Плохо	Низкий уровень знаний и несоблюдение правил безопасности. Нуждается в срочном обучении.	Провести срочное обучение по основным правилам безопасности. Назначить ответственного за контроль соблюдения правил безопасности.

ЗАДАНИЕ 16: АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ МАЛОГО БИЗНЕСА

Цель: научиться выявлять и описывать риски информационной безопасности, характерные для малого бизнеса, и разрабатывать рекомендации по их снижению.

Описание:

1. Выбор отрасли: выберите конкретную отрасль малого бизнеса, например, кафе, парикмахерская, небольшой интернет-магазин.

2. Определение активов: перечислите основные информационные активы, которыми владеет выбранный вами малый бизнес.

Примеры:

- Данные клиентов (имена, адреса, телефоны, email).
- База данных транзакций (информация о продажах, платежах).
- Финансовая информация (банковские счета, данные кредитных карт).
- Веб-сайт и учетные записи в социальных сетях.
- Компьютеры и ноутбуки сотрудников.
- Система учета товаров.
- Система онлайн-записи (для парикмахерской, например).

3. Идентификация угроз: для каждого актива из предыдущего пункта определите потенциальные угрозы, которые могут ему навредить.

Примеры:

- Вирусы и вредоносное ПО.
- Хакерские атаки.
- Фишинговые атаки.
- Утеря или кража оборудования.
- Ошибки сотрудников.
- Стихийные бедствия (пожар, наводнение).
- Инсайдерские угрозы (действия недобросовестных сотрудников).

4. Оценка рисков: для каждой пары «актив-угроза» оцените:

– Вероятность реализации угрозы: низкая, средняя, высокая.

– Потенциальный ущерб для бизнеса: незначительный, умеренный, серьезный.

5. Разработка рекомендаций: для каждой пары «актив-угроза» с высоким или средним уровнем риска разработайте конкретные рекомендации по снижению риска.

Примеры:

- Установка антивирусного ПО и его регулярное обновление.
- Регулярное резервное копирование данных.
- Использование надежных паролей и двухфакторной аутентификации.
- Обучение сотрудников основам информационной безопасности.
- Физическая защита оборудования (например, использование замков для ноутбуков).
- Разработка плана действий в чрезвычайных ситуациях.

6. Сделайте вывод о наиболее значимых рисках для выбранного малого бизнеса и о том, какие меры необходимо предпринять для обеспечения его информационной безопасности.

ЗАДАНИЕ 17: АНАЛИЗ ТРЕБОВАНИЙ К УПРАВЛЕНИЮ ДОСТУПОМ НА ОСНОВЕ СЦЕНАРИЯ

Цель: научиться анализировать сценарий деятельности организации и определять необходимые требования к управлению доступом для обеспечения безопасности информации.

Описание:

1. Изучение сценария: прочитайте следующий сценарий, описывающий деятельность гипотетической компании «БудьЗдоровВася», занимающейся обработкой медицинской информации:

«Компания БудьЗдоровВася предоставляет услуги по обработке и хранению медицинской информации для небольших клиник. Они используют облачную инфраструктуру для хранения данных пациентов и веб-приложение для доступа к этим данным. Сотрудники компании имеют разные роли: администраторы системы, врачи-консультанты, техническая поддержка. Врачи-консультанты могут просматривать медицинские записи пациентов, но не имеют права их изменять. Техническая поддержка может только просматривать логи системы для устранения проблем, но не имеет доступа к данным пациентов. Администраторы системы имеют полный доступ ко всем данным и системам, но обязаны соблюдать строгие правила безопасности».

2. Определение требований к управлению доступом: на основе анализа сценария определите требования к управлению доступом, которые необходимо реализовать в «БудьЗдоровВася» для обеспечения безопасности информации. Разделите требования на следующие категории:

– Идентификация и аутентификация:
  - Как идентифицируются пользователи?
  - Какие методы аутентификации используются?
  - Как обеспечивается надежность аутентификации?

– Авторизация:
  - Какие права доступа предоставляются разным ролям пользователей?
  - Как обеспечивается принцип наименьших привилегий (least privilege)?
  - Как контролируется доступ к конфиденциальным данным?
– Управление учетными записями:
  - Как создаются и удаляются учетные записи пользователей?
  - Как изменяются права доступа пользователей?
  - Как обеспечивается безопасность учетных записей привилегированных пользователей?
– Мониторинг и аудит:
  - Как ведется журнал доступа к данным и системам?
  - Как проводится аудит системы управления доступом?
  - Как выявляются и расследуются нарушения политики доступа?

3. Сделайте вывод о том, какие требования к управлению доступом являются наиболее важными для компании «БудьЗдоровВася» с учетом специфики ее деятельности и о том, какие риски могут возникнуть в случае несоблюдения этих требований.

ЗАДАНИЕ 18: РАЗРАБОТКА ЧЕК-ЛИСТА ДЛЯ ОЦЕНКИ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ СЕРВЕРНОЙ КОМНАТЫ

Цель: научиться разрабатывать чек-листы для проведения аудита физической безопасности серверной комнаты.

Описание:

1. Изучение требований к физической безопасности: изучите основные требования к физической безопасности серверной комнаты, например:

– Контроль доступа (ограничение доступа посторонних лиц).

– Система видеонаблюдения.

– Система пожаротушения.

– Система контроля климата (температура, влажность).

– Резервное электроснабжение.

– Защита от затопления.

– Защита от электромагнитных помех.

2. Разработка чек-листа: разработайте чек-лист для оценки физической безопасности серверной комнаты, включающий вопросы, позволяющие оценить соответствие серверной комнаты требованиям безопасности. Вопросы должны быть сформулированы таким образом, чтобы на них можно было ответить "да" или "нет", или выбрать один из нескольких вариантов ответа.

Примеры вопросов:

- Ограничен ли доступ в серверную комнату только для авторизованных лиц?
- Имеется ли система видеонаблюдения в серверной комнате?
- Функционирует ли система пожаротушения в серверной комнате?
- Поддерживается ли в серверной комнате стабильная температура и влажность?
- Имеется ли резервный источник электроснабжения (UPS или генератор)?

- Принимаются ли меры для защиты от затопления (например, поднятие оборудования над уровнем пола)?
- Заземлено ли оборудование для защиты от электростатических разрядов?
- Имеется ли план эвакуации на случай пожара или другой чрезвычайной ситуации?
- Проводятся ли регулярные проверки работоспособности систем безопасности?

3. Добавление комментариев: для каждого вопроса в чек-листе добавьте поле для комментариев, в котором можно указать дополнительную информацию или пояснения.

4. Сделайте вывод о том, какие аспекты физической безопасности серверной комнаты являются наиболее важными и о том, как разработанный чек-лист может помочь в проведении аудита и выявлении слабых мест.

ЗАДАНИЕ 19: ОБЗОР ТРЕБОВАНИЙ БЕЗОПАСНОСТИ ДЛЯ ВЫБРАННОЙ ОТРАСЛИ

Цель: получить базовое понимание о том, какие требования безопасности предъявляются к информационным системам в конкретной отрасли.

Описание:

1. Выбор отрасли: выберите одну из следующих отраслей:

   – Здравоохранение (медицинские клиники, больницы).

   – Финансовые услуги (банки, страховые компании).

   – Розничная торговля (интернет-магазины, супермаркеты).

   – Образование (школы, университеты).

2. Поиск требований безопасности: найдите информацию о требованиях безопасности, которые регулируют информационные системы в выбранной отрасли. Используйте следующие ресурсы:

   – Законодательство: ищите законы, постановления и нормативные акты, касающиеся защиты данных и информационной безопасности в выбранной отрасли в России.

   – Стандарты: ищите общепринятые стандарты безопасности, которые часто используются в выбранной отрасли.

   – Рекомендации: ищите рекомендации от отраслевых организаций, государственных органов или экспертов по информационной безопасности, касающиеся защиты данных и систем в выбранной отрасли.

3. Обобщение требований: составьте список наиболее важных требований безопасности для выбранной отрасли. Сгруппируйте требования по категориям, например:

   – Защита персональных данных: например, согласие на обработку данных, право на удаление данных, уведомление об утечках данных.

   – Контроль доступа: например, надежная аутентификация, ограничение доступа к данным.

– Защита от вредоносного ПО: например, использование антивирусного ПО, регулярное сканирование систем.

– Резервное копирование и восстановление данных: например, регулярное создание резервных копий, проверка возможности восстановления данных.

– Физическая безопасность: например, защита серверных помещений от несанкционированного доступа.

4. Примеры реализации: Для каждого требования безопасности из предыдущего пункта приведите пример того, как это требование может быть реализовано на практике.

5. Кратко опишите, какие особенности выбранной отрасли определяют предъявляемые к ней требования безопасности. Объясните, почему важно соблюдать эти требования.

ЗАДАНИЕ 20: РАЗРАБОТКА ПОЛИТИКИ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ГИПОТЕТИЧЕСКОЙ КОМПАНИИ

Цель: закрепить знания о принципах управления рисками и научиться разрабатывать политику управления рисками информационной безопасности (ИБ), как один из ключевых документов для сертификации ИС.

Описание:

1. Создание профиля компании: необходимо придумать и описать гипотетическую компанию. Обязательно укажите:

– Название компании.

– Отрасль деятельности (например, IT-консалтинг, финансовый сектор, здравоохранение, ритейл, производство). Обоснуйте выбор отрасли.

– Размер компании (количество сотрудников).

– Основные виды деятельности и бизнес-процессы.

– Ключевые информационные активы (например, данные клиентов, финансовая информация, интеллектуальная собственность, веб-сайт, ИТ-инфраструктура). Укажите, какие активы наиболее критичны для компании и почему.

– Требования соответствия стандартам и регуляторным нормам (например, Федеральный закон №152-ФЗ "О персональных данных").

2. Разработка политики управления рисками ИБ: Разработайте политику управления рисками информационной безопасности для созданной вами компании. Политика должна включать следующие разделы:

– Цель политики: четко сформулируйте цель политики. Например: «Целью данной политики является установление принципов и правил управления рисками информационной безопасности в компании [Название компании] для защиты ее информационных активов, обеспечения непрерывности бизнеса и соответствия требованиям законодательства и нормативных актов».

– Область применения: определите, на какие подразделения, процессы и информационные активы распространяется действие политики. Например: «Действие настоящей политики распространяется на все подразделения компании [Название компании], всех сотрудников, а также на все информационные активы, включая данные клиентов, финансовую информацию, интеллектуальную собственность, веб-сайт и ИТ-инфраструктуру».

– Определения и термины: приведите определения основных терминов, используемых в политике. Например: «Риск информационной безопасности, угроза, уязвимость, актив, ущерб».

– Принципы управления рисками: перечислите основные принципы управления рисками, которые компания будет соблюдать. Например: «Принцип ответственности, принцип непрерывности, принцип пропорциональности, принцип прозрачности».

– Роли и ответственности: определите роли и ответственности сотрудников, участвующих в процессе управления рисками. Например:

- «Руководство компании: несет ответственность за общее руководство процессом управления рисками и выделение необходимых ресурсов».
- «Отдел информационной безопасности: отвечает за разработку и внедрение методологии управления рисками, проведение оценки рисков, разработку планов управления рисками и мониторинг их выполнения».
- «Владельцы активов: несут ответственность за защиту своих активов и участие в процессе оценки рисков».
- «Все сотрудники: несут ответственность за соблюдение правил и политик информационной безопасности и сообщают об обнаруженных инцидентах и уязвимостях».

– Методология оценки рисков: опишите методологию, которую компания будет использовать для оценки рисков. Например: «Компания [Название компании] будет использовать качественную методологию оцен-

ки рисков, основанную на определении вероятности и ущерба от реализации рисков».

– Процесс управления рисками: опишите основные этапы процесса управления рисками:

– Идентификация рисков: определение потенциальных угроз и уязвимостей.

– Оценка рисков: определение вероятности и ущерба от реализации рисков.

– Обработка рисков: выбор и реализация мер по снижению или устранению рисков.

– Мониторинг и пересмотр: постоянный мониторинг эффективности мер по управлению рисками и их пересмотр при необходимости.

– Меры контроля: перечислите основные меры контроля, которые компания будет использовать для снижения рисков. Например: «Технические меры контроля (межсетевые экраны, системы обнаружения вторжений, антивирусное ПО), организационные меры контроля (политики и процедуры безопасности, обучение персонала), физические меры контроля (ограничение доступа в серверную комнату)».

– Мониторинг и пересмотр: опишите порядок мониторинга и пересмотра политики управления рисками. Например: «Политика управления рисками должна пересматриваться не реже одного раза в год или при существенных изменениях в бизнес-процессах, ИТ-инфраструктуре или законодательстве».

– Ответственность за соблюдение: укажите, кто несет ответственность за соблюдение политики.

– Ответственность за соблюдение настоящей политики несут все сотрудники компании [Название компании].

– Действия в случае нарушения: определите действия, которые будут предприняты в случае нарушения политики.

– В случае нарушения настоящей политики к сотрудникам могут быть применены дисциплинарные взыскания, вплоть до увольнения.

– Дата вступления в силу и срок действия: укажите дату вступления в силу и срок действия политики.

– Утверждение: укажите, кто утверждает политику.

3. Опишите, как разработанная политика управления рисками поможет компании в обеспечении информационной безопасности и подготовке к сертификации ИС.

ЗАДАНИЕ 21: ПРОВЕДЕНИЕ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ВЫБРАННОГО ИНФОРМАЦИОННОГО АКТИВА

Цель: применить на практике знания о методах идентификации и оценки рисков ИБ.

Описание:

1. Выбор информационного актива: выберите один из ключевых информационных активов, указанных в задании 1, для вашей гипотетической компании. Например, это может быть база данных клиентов, веб-сайт, система электронного документооборота или облачное хранилище данных.

2. Идентификация угроз: определите потенциальные угрозы, которые могут нанести ущерб выбранному информационному активу. Используйте различные методы идентификации угроз, такие как:

   – Анализ документации (например, анализ отчетов о предыдущих инцидентах безопасности, анализ архитектуры системы).

   – Интервью с заинтересованными сторонами (например, интервью с владельцем актива, системным администратором, специалистом по безопасности).

   – Использование списков типовых угроз (например, списки угроз OWASP для веб-приложений).

   – Мозговой штурм (brainstorming).

3. Идентификация уязвимостей: определите уязвимости выбранного информационного актива, которые могут быть использованы угрозами. Используйте различные методы идентификации уязвимостей, такие как:

   – Сканирование уязвимостей.

   – Тестирование на проникновение.

   – Анализ кода (code review).

   – Проверка конфигурации системы.

4. Оценка вероятности: оцените вероятность реализации каждой идентифицированной угрозы для выбранного актива. Используйте качественную или количественную оценку вероятности (например, низкая, средняя, высокая или 1-10). Обоснуйте свою оценку для каждой угрозы. Учитывайте наличие существующих мер контроля.

5. Оценка ущерба: оцените потенциальный ущерб, который может быть нанесен организации в случае реализации каждой угрозы для выбранного актива. Используйте качественную или количественную оценку ущерба (например, незначительный, умеренный, серьезный или в денежном выражении). Обоснуйте свою оценку для каждой угрозы.

6. Определение уровня риска: определите уровень риска для каждой пары «угроза-уязвимость» на основе сочетания вероятности и ущерба. Используйте матрицу рисков (как в примере в предыдущих ответах) или другую подходящую методику.

7. Приоритизация рисков: приоритизируйте риски на основе их уровня. Определите, какие риски требуют немедленного внимания и какие могут быть отложены.

8. Опишите, какие риски являются наиболее критичными для выбранного информационного актива и какие меры необходимо предпринять для их снижения.

ЗАДАНИЕ 22: РАЗРАБОТКА ПЛАНА УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ВЫБРАННОГО РИСКА

Цель: научиться разрабатывать конкретные планы управления рисками, включающие выбор и внедрение мер контроля.

Описание:

1. Выбор риска: выберите один из рисков, идентифицированных в предыдущих заданиях, с высоким или критическим уровнем риска.

2. Определение стратегии управления риском: выберите стратегию управления выбранным риском: избежание, снижение, перенос или принятие. Обоснуйте свой выбор.

3. Выбор мер контроля: определите конкретные меры контроля, которые необходимо внедрить для реализации выбранной стратегии. Обоснуйте выбор каждой меры контроля. Учитывайте различные типы мер контроля (организационные, технические, физические). Примеры мер контроля:

– Разработка и внедрение политики парольной защиты.

– Установка межсетевого экрана (firewall).

– Внедрение системы обнаружения вторжений.

– Проведение обучения сотрудников правилам информационной безопасности.

– Резервное копирование данных.

– Шифрование данных.

– Внедрение системы управления доступом.

– Ограничение физического доступа к серверной комнате.

4. Разработка плана внедрения мер контроля: разработайте план внедрения выбранных мер контроля. План должен включать следующие элементы:

– Описание задачи: конкретное описание меры контроля, которую необходимо внедрить.

– Ответственный: сотрудник или отдел, ответственный за внедрение меры контроля.

– Сроки: срок начала и окончания внедрения меры контроля.

– Ресурсы: необходимые ресурсы для внедрения меры контроля (например, бюджет, оборудование, программное обеспечение, время сотрудников).

– Критерии успеха: критерии, которые будут использоваться для оценки эффективности внедрения меры контроля.

5. Разработка плана мониторинга мер контроля: разработайте план мониторинга эффективности внедренных мер контроля. План должен включать следующие элементы:

– Описание задачи: описание действий, которые необходимо предпринять для мониторинга эффективности меры контроля.

– Ответственный: сотрудник или отдел, ответственный за мониторинг меры контроля.

– Сроки: периодичность мониторинга (например, ежедневно, еженедельно, ежемесячно).

– Метрики: метрики, которые будут использоваться для оценки эффективности меры контроля (например, количество инцидентов безопасности, количество заблокированных атак, время восстановления системы после сбоя).

6. Оценка остаточного риска: оцените уровень остаточного риска после внедрения мер контроля.

7. Опишите, насколько эффективно разработанный план управления рисками поможет снизить выбранный риск и какие факторы могут повлиять на его успешную реализацию.

ЗАДАНИЕ 23: РАЗРАБОТКА КОМПЛЕКТА ДОКУМЕНТОВ ДЛЯ ГИПОТЕТИЧЕСКОЙ КОМПАНИИ, ГОТОВЯЩЕЙСЯ К СЕРТИФИКАЦИИ

Цель: закрепить знания о видах документов, необходимых для сертификации ИС, и научиться разрабатывать основные документы, соответствующие выбранному стандарту сертификации.

Описание:

1. Создание профиля компании: разработайте профиль гипотетической компании, аналогично заданию 1 из предыдущего набора заданий (укажите название, отрасль деятельности, размер, основные виды деятельности, ключевые информационные активы и главное – стандарт, по которому планируется сертификация и почему).

2. Выбор документов: на основе выбранного стандарта сертификации, определите 3-4 ключевых документа, которые необходимо разработать для успешной сертификации. Примеры документов:

– Политика информационной безопасности (обязательно!).

– Инструкция по управлению доступом к информационным системам.

– Инструкция по резервному копированию и восстановлению данных.

– Регламент использования электронной почты.

– План реагирования на инциденты безопасности (для конкретного сценария, например, утечка данных).

– Процедура управления изменениями.

3. Разработка документов: разработайте выбранные документы, соблюдая следующие требования:

– Соответствие стандарту: документы должны соответствовать требованиям выбранного стандарта сертификации. Укажите в каждом документе, каким конкретно требованиям стандарта он соответствует.

– Полнота и точность: документы должны содержать всю необходимую информацию для понимания процессов и процедур информационной безопасности.

– Актуальность: информация в документах должна быть точной и соответствовать реальному положению дел.

– Утверждение и согласование: укажите, кто должен утверждать и согласовывать каждый документ в вашей гипотетической компании (например, генеральный директор, руководитель отдела ИБ, юрист).

– Форматирование: используйте стандартизованные форматы документов и шаблоны.

4. Обоснование выбора: для каждого разработанного документа, предоставьте краткое обоснование, почему он важен для подготовки к сертификации и каким требованиям выбранного стандарта он соответствует.

5. Опишите, как разработанные документы помогут компании в подготовке к сертификации ИС и продемонстрировать соответствие требованиям выбранного стандарта.

ЗАДАНИЕ 24: АНАЛИЗ СУЩЕСТВУЮЩЕЙ ДОКУМЕНТАЦИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ВЫЯВЛЕНИЕ НЕСООТВЕТСТВИЙ ТРЕБОВАНИЯМ СТАНДАРТА СЕРТИФИКАЦИИ

Цель: научиться анализировать существующую документацию по информационной безопасности (ИБ) и выявлять несоответствия требованиям стандартов сертификации, критически важный навык для успешного прохождения сертификационного аудита.

Описание:

1. Выбор стандарта и компании: выберите один из стандартов сертификации. Создайте (или используйте из предыдущего задания) профиль гипотетической компании, для которой будет проводиться анализ (укажите стандарт сертификации, отрасль, размер и т.д.).

2. Поиск образцов документации: найдите в открытых источниках (например, на сайтах консалтинговых компаний по ИБ, в библиотеках шаблонов, в примерах, предоставленных стандартами) 2-3 примера документов по ИБ, которые гипотетически использует ваша компания. Это могут быть, например:

– Политика информационной безопасности (разных компаний).

– Инструкция по созданию паролей (разных компаний).

– План реагирования на инциденты (разных компаний).

3. Анализ документации: проанализируйте найденные документы на соответствие требованиям выбранного стандарта сертификации. Для каждого документа, выявите:

– Соответствия: какие требования стандарта выполняются в документе? Укажите конкретные пункты стандарта.

– Несоответствия: какие требования стандарта не выполняются в документе? Укажите конкретные пункты стандарта.

– Области для улучшения: какие разделы документа можно улучшить, чтобы повысить соответствие требованиям стандарта?

– Отсутствующие элементы: какие важные элементы отсутствуют в документе, которые необходимы для соответствия стандарту?

4. Оформление результатов анализа: Результаты анализа для каждого документа оформите в виде таблицы или списка, с указанием конкретных пунктов стандарта, соответствий, несоответствий и рекомендаций по улучшению.

5. Сделайте выводы о том, какие общие проблемы и недостатки характерны для документации по ИБ и как их можно избежать при подготовке к сертификации ИС.

ЗАДАНИЕ 25: РАЗРАБОТКА ПЛАНА АКТУАЛИЗАЦИИ ДОКУМЕНТАЦИИ ПО ИБ ДЛЯ ПРОХОЖДЕНИЯ СЕРТИФИКАЦИОННОГО АУДИТА

Цель: научиться разрабатывать конкретный план действий по актуализации документации ИБ, чтобы успешно пройти сертификационный аудит, понимая, что документы «сами по себе» не работают, нужен план.

Описание:

1. Выбор компании и стандарта: используйте профиль гипотетической компании и стандарт сертификации, выбранные в предыдущих заданиях. Предположим, что компания провела первоначальную оценку готовности к сертификации и выявила ряд проблем с документацией (можно использовать результаты анализа из предыдущих заданий).

2. Определение задач по актуализации: на основе выявленных проблем с документацией, определите конкретные задачи по актуализации документации, которые необходимо выполнить для успешного прохождения сертификационного аудита. Примеры задач:

   – Разработка недостающих документов (например, разработать план реагирования на инциденты утечки данных).

   – Обновление существующих документов (например, обновить политику информационной безопасности в соответствии с последней версией стандарта).

   – Проведение обучения персонала работе с документацией.

   – Внедрение системы контроля версий.

   – Согласование документов с заинтересованными сторонами.

3. Разработка плана-графика: разработайте план-график выполнения задач по актуализации документации. План-график должен включать следующие элементы:

– Задача: описание конкретной задачи.

– Ответственный: сотрудник или отдел, ответственный за выполнение задачи.

– Срок начала: дата начала выполнения задачи.

– Срок окончания: дата окончания выполнения задачи.

– Ресурсы: необходимые ресурсы для выполнения задачи (например, бюджет, время сотрудников, консультанты).

– Статус: текущий статус выполнения задачи (например, запланировано, в процессе, выполнено, отложено).

– Зависимости: укажите, от выполнения каких других задач зависит выполнение данной задачи.

4. Определение критериев успеха: для каждой задачи, определите конкретные критерии успеха, которые будут использоваться для оценки эффективности выполнения задачи. Например:

– Задача: «Разработать план реагирования на инциденты утечки данных».

– Критерии успеха: «План разработан, утвержден руководством, согласован с юридическим отделом, протестирован в ходе учений».

Опишите, как разработанный план поможет компании успешно подготовиться к сертификационному аудиту и продемонстрировать готовность к сертификации ИС. Укажите, какие факторы могут повлиять на успешную реализацию плана и какие меры необходимо предпринять для их учета.

ВОПРОСЫ К ЭКЗАМЕНУ ПО КУРСУ «СЕРТИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ»

Лекция 1: Введение в сертификацию информационных систем

1. Что такое сертификация информационных систем (ИС)?
2. Каковы основные цели сертификации ИС?
3. Перечислите преимущества сертификации ИС для организации.
4. Какие существуют типы сертификации ИС (например, обязательная и добровольная)?
5. В чем разница между сертификацией продукции и сертификацией систем управления информационной безопасностью (СУИБ)?
6. Назовите основные заинтересованные стороны в процессе сертификации ИС.
7. Объясните понятия "орган по сертификации", "заявитель" и "аудитор".
8. Что такое область сертификации и как она определяется?

Лекция 2: Нормативная база и стандарты сертификации ИС

9. Какие основные нормативные акты регулируют сертификацию ИС в России?
10. Что такое стандарт сертификации и какова его роль в процессе сертификации ИС?
11. Какие основные стандарты и нормативные документы используются в России для обеспечения безопасности информационных систем?
12. Объясните, какие разделы обычно содержит стандарт (или нормативный документ) по информационной безопасности и что описывается в каждом из этих разделов.
13. Какие основные требования к безопасности предъявляются российским организациям, обрабатывающим данные платежных карт, в соответствии с требованиями международных платежных систем и нормативных актов, таких

как стандарт PCI DSS (применимый на добровольной основе) и рекомендации Банка России?

14. Какие основные принципы защиты персональных данных определены в российском законодательстве, в частности, в Федеральном законе № 152-ФЗ "О персональных данных"?

15. Чем отличаются национальные стандарты сертификации ИС от международных?

16. Объясните понятие "гармонизация стандартов".

17. Что такое аккредитация органов по сертификации и какова ее цель?

Лекция 3: Объекты сертификации информационных систем

18. 1Что может являться объектом сертификации в сфере ИС? Приведите примеры.

19. В чем разница между сертификацией программного обеспечения и сертификацией аппаратного обеспечения?

20. Какие компоненты СУИБ могут быть сертифицированы?

21. Что такое "услуги по информационной безопасности" и могут ли они быть сертифицированы?

22. Какие особенности сертификации облачных сервисов?

23. Как определяется область сертификации для конкретного объекта?

24. Какие факторы следует учитывать при выборе объекта сертификации?

Лекция 4: Процесс сертификации: от подачи заявки до получения сертификата

25. Опишите основные этапы процесса сертификации ИС.

26. Какие документы необходимо предоставить в орган по сертификации при подаче заявки?

27. Что такое предварительный аудит и какова его цель?

28. В чем разница между аудитом первой и второй стадии?

29. Какие действия предпринимает орган по сертификации, если в ходе аудита выявлены несоответствия?

30. Что такое корректирующие действия и какова их цель?

31. Как принимается решение о выдаче сертификата соответствия?

32. Каков срок действия сертификата соответствия?

33. Что такое надзорный аудит и какова его цель?

34. Опишите процесс сертификации.

Лекция 5: Методы и средства контроля при сертификации ИС

35. Какие методы контроля используются при сертификации ИС?

36. Что такое анализ документации и какова его цель?

37. В чем заключается проверка соответствия требованиям безопасности?

38. Что такое тестирование и какие виды тестирования применяются при сертификации ИС?

39. Какова роль интервью с персоналом в процессе сертификации ИС?

40. Какие технические средства контроля используются при сертификации ИС (например, сканеры уязвимостей, системы обнаружения вторжений)?

41. Что такое "политики", "процедуры" и "инструкции" и как они проверяются в процессе сертификации?

Лекция 6: Аудит информационной безопасности как этап сертификации

42. Что такое аудит информационной безопасности и какова его цель?

43. Какие существуют виды аудита информационной безопасности (например, внутренний и внешний)?

44. Опишите этапы проведения аудита информационной безопасности.

45. Каковы основные задачи аудитора информационной безопасности?

46. Какие навыки и компетенции необходимы аудитору информационной безопасности?

47. Что такое аудиторское заключение и каково его содержание?

48. В чем разница между аудитом соответствия и аудитом производительности?

Лекция 7: Управление рисками и их роль в сертификации ИС

49. Что такое риск в контексте информационной безопасности?

50. Опишите основные этапы процесса управления рисками.

51. Какие существуют методы оценки рисков (например, качественная и количественная)?

52. Что такое матрица рисков и как она используется?

53. Какие существуют стратегии обработки рисков (например, избежание, снижение, передача, принятие)?

54. Как результаты оценки рисков используются при выборе мер контроля для СУИБ?

55. Какова роль управления рисками в процессе сертификации ИС?

Лекция 8: Практические аспекты подготовки к сертификации (документация)

56. Какие документы необходимы для успешной сертификации ИС?

57. Каковы основные требования к документации по ИБ (например, полнота, точность, актуальность)?

58. Какие практические рекомендации можно дать по составлению и поддержанию документации по ИБ?

ЗАКЛЮЧЕНИЕ

Практикум «Практические задания по дисциплине «Сертификация информационных систем»» является важным элементом практико-ориентированной подготовки студентов специальности 09.02.07 «Информационные системы и программирование». Он позволяет сформировать у обучающихся понимание роли сертификации в обеспечении доверия и безопасности информационных систем, закрепить теоретические знания через выполнение прикладных заданий, а также развить навыки анализа, планирования и подготовки необходимой документации, связанной с процедурами сертификации.

Выполнение заданий, представленных в практикуме, способствует:

- овладению методами анализа информационных систем и идентификации угроз информационной безопасности;
- изучению законодательных и нормативных основ, регламентирующих процессы сертификации в Российской Федерации;
- освоению практических подходов к подготовке и проведению сертификационных испытаний и аудита;
- приобретению умений разрабатывать политики информационной безопасности и планы сертификации;
- подготовке к самостоятельному решению задач по сертификации ИС в рамках профессиональной деятельности.

Практическая направленность методического пособия даёт возможность студентам ознакомиться с актуальными требованиями регуляторов (ФСТЭК, ФСБ, Минцифры России), а также международными стандартами (ISO/IEC 27001, 27002) через выполнение кейсов и анализ реальных и имитационных сценариев.

Применение данного практикума в образовательном процессе позволит:

- качественно подготовить студентов к профессиональной деятельности в области информационных технологий и информационной безопасности;

- развить компетенции в части соблюдения требований к безопасности и сертификации информационных систем;
- сформировать ответственное отношение к процессам защиты информации и прав пользователей информационных систем.

Практикум может использоваться как в рамках аудиторных занятий, так и для самостоятельной работы студентов, а также в качестве инструмента для организации текущего и итогового контроля знаний и практических навыков.

Комплексное освоение материалов данного практикума позволит студентам не только успешно изучить дисциплину «Сертификация информационных систем», но и подготовит их к практическому применению полученных знаний в профессиональной деятельности в условиях современного ИТ-рынка и требований цифровой экономики.

ОПИСАНИЕ ФУНКЦИОНАЛЬНОСТИ ИЗДАНИЯ:

Интерфейс электронного издания (в формате pdf) можно условно разделить на 2 части.

Левая навигационная часть (закладки) включает в себя содержание книги с возможностью перехода к тексту соответствующей главы по левому щелчку компьютерной мыши.

Центральная часть отображает содержание текущего раздела. В тексте могут использоваться ссылки, позволяющие более подробно раскрыть содержание некоторых понятий.

МИНИМАЛЬНЫЕ СИСТЕМНЫЕ ТРЕБОВАНИЯ:

Celeron 1600 Mhz; 128 Мб RAM; Windows XP/7/8 и выше; 8x DVD-ROM; разрешение экрана 1024×768 или выше; программа для просмотра pdf.

СВЕДЕНИЯ О ЛИЦАХ, ОСУЩЕСТВЛЯВШИХ ТЕХНИЧЕСКУЮ ОБРАБОТКУ И ПОДГОТОВКУ МАТЕРИАЛОВ:

Оформление электронного издания : Издательский центр «Удмуртский университет».

Авторская редакция

Подписано к использованию 30.12.2025
Объем электронного издания 1 Мб
Издательский центр «Удмуртский университет»
426034, г. Ижевск, ул. Ломоносова, д. 4Б, каб. 021
Тел. : +7(3412)916-364 E-mail: editorial@udsu.ru