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

Методические указания

по выполнению практических занятий
по дисциплине
«Организационное и правовое обеспечение информационной безопасности»
для студентов
Специальности 10.05.03 Информационная безопасность
автоматизированных систем
Специализация «Анализ безопасности информационных систем»

Ставрополь
2026

Семестр 7

Практическая работа 1: Анализ структуры и нормативной базы компании в сфере информационной безопасности

Цель работы: Изучить организационную структуру компании, определить ключевые нормативные документы, регулирующие информационную безопасность, и проанализировать их соответствие требованиям законодательства.

1. Теоретическая часть

1.1. Организационная структура компании

Компании в сфере ИБ могут иметь разные структуры:

Линейная – подходит для небольших организаций.

Функциональная – разделение по направлениям (например, отделы SOC, pentest, compliance).

Матричная – гибридная структура для крупных компаний.

1.2. Нормативная база

Основные документы, регулирующие ИБ в компании:

Внутренние:

Политика информационной безопасности.

Регламенты и инструкции по работе с данными.

Положение о коммерческой тайне.

Внешние (законодательные):

ФЗ №152 "О персональных данных" (для РФ).

GDPR (для работы с ЕС).

ISO 27001 – международный стандарт ИБ.

PCI DSS – для компаний, работающих с платежами.

2. Практическое задание

Задание 1. Анализ структуры компании

Выберите реальную или гипотетическую компанию (например, банк, IT-стартап, госучреждение).

Определите её структуру (линейная, функциональная и т. д.).

Выделите отделы, отвечающие за ИБ (например, SOC, отдел compliance, служба DLP).

Пример заполнения:

Компания	Банк "РусФинанс"
Тип структуры	Функциональная
Отделы, связанные с ИБ	1. Отдел кибербезопасности (SOC). 2. Отдел compliance. 3. Служба реагирования на инциденты (CSIRT).

Задание 2. Анализ нормативной базы

Изучите, какие внутренние и внешние документы регулируют ИБ в выбранной компании.

Проверьте, соответствует ли политика компании законодательству (например, ФЗ №152).

Пример заполнения:

Нормативный документ	Соответствует закону? (Да/Нет)	Примечание
Политика ИБ банка "РусФинанс"	Да	Соответствует ФЗ №152 и PCI DSS.
Инструкция по обработке ПДн	Нет	Нет механизма уведомления клиентов об утечках.

Задание 3. Рекомендации по улучшению

- На основе выявленных несоответствий предложите меры:
- Внести изменения в инструкцию по ПДн.
- Провести аудит на соответствие ISO 27001.

3. Вопросы для самоконтроля

- Какие отделы обычно отвечают за ИБ в крупной компании?
- Назовите 3 ключевых закона, регулирующих ИБ в РФ.
- Почему важно соответствие стандарту ISO 27001?

Нормативно-правовые акты РФ

1. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
2. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
3. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
4. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

1. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
2. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
3. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

1. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
2. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
3. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

1. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
2. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
3. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 2: Законодательство РФ в области информационной безопасности

Цель работы: Изучить основные законы и нормативные акты РФ, регулирующие информационную безопасность (ИБ), и научиться применять их на практике.

1. Теоретическая часть

1.1. Основные законы РФ в сфере ИБ
Федеральный закон № 149-ФЗ "Об информации, информационных технологиях и о защите информации"
Определяет понятия информации, её категории (общедоступная, конфиденциальная).
Регулирует порядок защиты информации.
Федеральный закон № 152-ФЗ "О персональных данных"
Устанавливает требования к обработке ПДн.
Обязанности операторов ПДн (уведомление Роскомнадзора, защита данных).
Федеральный закон № 187-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)"
Регулирует защиту объектов КИИ (банки, энергетика, транспорт).
Обязывает организации внедрять системы защиты.
Федеральный закон № 98-ФЗ "О коммерческой тайне"
Определяет порядок защиты конфиденциальной информации в бизнесе.
Указ Президента РФ № 400 "О стратегии национальной безопасности"

Включает кибербезопасность как элемент нацбезопасности.
Стандарты и ГОСТы:
ГОСТ Р 57580.1–2017 (требования к банковской безопасности).
СТБ (Стандарты Банка России) для финансового сектора.

2. Практическая часть
Задание 1. Анализ законодательных требований
Шаг 1. Выберите организацию (банк, госучреждение, интернет-магазин).
Шаг 2. Определите, какие законы из списка выше к ней применяются.

Пример заполнения:

Организация	Применяемые законы	Обоснование
Банк "Альфа-Банк"	152-ФЗ, 187-ФЗ, 98-ФЗ, ГОСТ Р 57580.1	Обрабатывает ПДн, относится к КИИ, хранит коммерческую тайну.

Задание 2. Проверка соответствия законодательству
Ситуация: Интернет-магазин хранит данные клиентов (ФИО, телефоны, адреса).
Вопросы:
Какой закон обязывает защищать эти данные?
Нужно ли уведомлять Роскомнадзор?
Какие меры защиты должны быть?
Задание 3. Разбор кейса
Кейс: Компания не зарегистрировалась как оператор ПДн, но собирает данные клиентов.
Задача:
Какие нарушения?
Какие штрафы по ст. 13.11 КоАП?
Как исправить?
3. Вопросы для самоконтроля
Назовите 3 закона, регулирующих защиту ПДн в РФ.
Какие организации относятся к КИИ?
Что грозит компании за утечку ПДн?

Нормативно-правовые акты РФ

5. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
6. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
7. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
8. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

4. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
5. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
6. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

4. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
5. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
6. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

4. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
5. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
6. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 3: Нормативно-правовые акты. ФЗ «О техническом регулировании» в сфере информационной безопасности

Цель работы:
Изучить Федеральный закон № 184-ФЗ «О техническом регулировании», его роль в стандартизации и обеспечении информационной безопасности (ИБ), а также научиться применять его положения на практике.

1. Теоретическая часть

1.1. Основные положения ФЗ № 184-ФЗ
Федеральный закон «О техническом регулировании» регулирует:
Разработку и применение технических регламентов (обязательные требования к продукции и процессам).
Применение национальных стандартов (ГОСТ Р) и международных стандартов.

Принципы оценки соответствия (сертификация, декларирование).
1.2. Связь с информационной безопасностью
Закон влияет на ИБ через:
Технические регламенты, например:
ТР ТС 004/2011 (безопасность низковольтного оборудования, включая ИТ-устройства).
ТР ТС 020/2011 (электромагнитная совместимость техники).
ГОСТы в ИБ:
ГОСТ Р 57580.1–2017 (безопасность финансовых организаций).
ГОСТ Р ИСО/МЭК 27001 (системы менеджмента ИБ).

2. Практические задания

Задание 1. Анализ применения ФЗ № 184-ФЗ в ИБ
Шаг 1. Выберите организацию (банк, госучреждение, облачный провайдер).
Шаг 2. Определите, какие технические регламенты и ГОСТы ей соответствуют.

Пример заполнения:

Организация	Применимые техрегламенты/ГОСТы	Обоснование
Банк "Сбербанк"	ТР ТС 004/2011, ГОСТ Р 57580.1, ГОСТ Р ИСО/МЭК 27001	Использует серверное оборудование (ТР ТС 004), подпадает под требования ЦБ РФ (ГОСТ 57580.1).

Задание 2. Разбор требований технического регламента
Ситуация: Компания разрабатывает сервер для госструктур.
Вопросы:
Какой техрегламент регулирует его безопасность?
Требуется ли обязательная сертификация?
Какие ГОСТы можно применить дополнительно?
Задание 3. Сравнение добровольных и обязательных стандартов
Задача:
Сравните ГОСТ Р ИСО/МЭК 27001 (добровольный) и ТР ТС 004/2011 (обязательный).
В каких случаях компания может выбрать только ГОСТ?
Пример ответа:

Критерий	ГОСТ Р ИСО/МЭК 27001	ТР ТС 004/2011
Обязательность	Добровольный	Обязательный
Применение	Любые организации	Производители оборудования
Цель	Улучшение ИБ	Соответствие безопасности продукции

Вывод:

3. Вопросы для самоконтроля

Назовите 2 технических регламента, связанных с ИБ.
Чем отличается ГОСТ от техрегламента?

Какие организации обязаны соблюдать ТР ТС 004/2011?

Нормативно-правовые акты РФ

9. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
10. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
11. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
12. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

7. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
8. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
9. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

7. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
8. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
9. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

7. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
8. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
9. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 4: Правовое регулирование отдельных видов информации в сфере информационной безопасности

Цель работы: Изучить особенности правового регулирования различных видов информации (государственная тайна, персональные данные, коммерческая тайна и др.), научиться анализировать нормативные акты и применять их на практике.

1. Теоретическая часть

1.1. Виды информации и их правовой статус
В РФ информация классифицируется по степени доступа и защиты:
Государственная тайна
Регулируется Законом РФ № 5485-1 «О государственной тайне».
Примеры: военные секреты, данные о внешней политике.
Персональные данные (ПДн)
Регулируются ФЗ № 152-ФЗ «О персональных данных».
Требования: согласие субъекта, защита от утечек.
Коммерческая тайна
Регулируется ФЗ № 98-ФЗ «О коммерческой тайне».
Примеры: ноу-хау, клиентские базы.
Конфиденциальная служебная информация
Регулируется Указом Президента № 188.
Примеры: данные следствия, врачебная тайна.
Общедоступная информация
Регулируется ФЗ № 149-ФЗ «Об информации...».
Примеры: новости, открытые госданные.
1.2. Ответственность за нарушение режима информации
Уголовная (ст. 283 УК РФ) – за разглашение гостайны.
Административная (ст. 13.14 КоАП РФ) – за нарушение конфиденциальности.
Гражданско-правовая – возмещение ущерба за утечку коммерческой тайны.

2. Практические задания

Задание 1. Определение вида информации и регулирующих актов
Шаг 1. Приведите примеры информации (3-4 случая).
Шаг 2. Определите, к какому виду она относится, и назовите регулирующий закон.
Пример заполнения:

Пример информации	Вид информации	Регулирующий акт
База данных клиентов банка	Персональные данные	ФЗ № 152-ФЗ
Чертежи нового военного дрона	Государственная тайна	Закон № 5485-1
Рецепт фирменного соуса KFC	Коммерческая тайна	ФЗ № 98-ФЗ

Задание 2. Анализ нарушений

Кейс 1: Сотрудник IT-компании скопировал исходный код проекта и продал конкурентам.
Вопросы:
Какой вид информации нарушен?
Какая ответственность грозит сотруднику?
Какие меры защиты должен был внедрить работодатель?
Кейс 2: Врач опубликовал в соцсетях историю болезни пациента.
Задание 3. Сравнительная таблица видов информации
Сравните государственную тайну, ПДн и коммерческую тайну по критериям:
Регулирующий закон.
Кто имеет доступ.
Наказание за разглашение.
Пример заполнения:

Критерий	Государственная тайна	Персональные данные	Коммерческая тайна
Закон	Закон № 5485-1	ФЗ № 152-ФЗ	ФЗ № 98-ФЗ
Доступ	Сотрудники с допуском ФСБ	Операторы ПДн	Работники по NDA
Ответственность	До 7 лет лишения свободы (ст. 283 УК)	Штраф до 75 000 руб. (ст. 13.11 КоАП)	До 7 лет (ст. 183 УК)

3. Вопросы для самоконтроля
Назовите 3 вида конфиденциальной информации.
Какой закон регулирует врачебную тайну?
Чем отличается коммерческая тайна от ПДн?

Нормативно-правовые акты РФ

13. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
14. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
15. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
16. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

10. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)

11. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
12. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

10. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
11. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
12. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

10. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
11. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
12. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 5: Правовое обеспечение защиты банковской, профессиональной и служебной тайны

Цель работы: Изучить правовые основы защиты специальных видов тайн (банковской, профессиональной, служебной), научиться анализировать нормативные акты и применять их в профессиональной деятельности.

1. Теоретическая часть

1.1. Виды защищаемой информации и их правовой статус
1.1.1. Банковская тайна
Определение: Сведения о клиентах, операциях, счетах и финансовом состоянии.
Нормативная база:
ФЗ №395-1 "О банках и банковской деятельности" (ст. 26)
ГК РФ (ст. 857)
Налоговый кодекс (ст. 84)
Субъекты доступа: Клиент, банк, ЦБ РФ, суды, ФНС (ограниченно).
Ответственность за разглашение:

Гражданско-правовая (возмещение ущерба)
Уголовная (ст. 183 УК РФ - до 7 лет лишения свободы)
1.1.2. Профессиональная тайна
Виды:
Врачебная
Адвокатская
Нотариальная
Регулирование:
Основы законодательства РФ об охране здоровья (ст. 13)
ФЗ №63 "Об адвокатской деятельности" (ст. 8)
Особенности: Не подлежит разглашению даже в суде (кроме исключений).
1.1.3. Служебная тайна
Определение: Информация, ставшая известной госорганам при исполнении обязанностей.
Регулирование:
Указ Президента №188 (перечень конфиденциальной информации)
ФЗ №79 "О госслужбе"
Примеры: Данные налоговых проверок, следственные материалы.
1.2. Сравнительная характеристика видов тайн

Критерий	Банковская тайна	Профессиональная тайна	Служебная тайна
Основной закон	ФЗ №395-1	Отраслевые законы	Указ №188
Субъекты	Банки, клиенты	Врачи, адвокаты	Госслужащие
Доступ третьих лиц	По решению суда	Почти невозможен	По запросу госорганов
Ответственность	Ст. 183 УК РФ	Дисциплинарная, уголовная	Ст. 283 УК РФ

---

2. Практические задания
Задание 1. Определение вида тайны
Даны ситуации:
Налоговый инспектор передал данные о доходах предпринимателя его конкуренту
Врач рассказал журналистам о диагнозе известного актера
Банковский сотрудник продал базу данных клиентов
Требуется:
Определить вид тайны
Указать нормативный акт
Предусмотренную ответственность
Пример ответа:

Ситуация	Вид тайны	Нормативный акт	Ответственность
1	Служебная	Указ №188	Ст. 13.14 КоАП (штраф до 5 000 руб)
2	Профессиональная (врачебная)	Основы законодательства об охране здоровья	Ст. 137 УК РФ (до 4 лет)
3	Банковская	ФЗ №395-1	Ст. 183 УК РФ (до 7 лет)

Задание 2. Анализ кейса
Ситуация: В кредитной организации произошла утечка данных: стали доступны номера счетов и паспортные данные клиентов.
Вопросы:
Какой вид тайны нарушен?
Какие нормативные акты были нарушены?
Какие меры защиты должны были быть реализованы?
Какая ответственность грозит банку?
Задание 3. Разработка мер защиты
Задача: Для медицинского центра разработать:
Перечень защищаемых сведений
Организационные меры защиты
Технические средства защиты

3. Вопросы для самоконтроля

Чем отличается банковская тайна от коммерческой?
Может ли адвокат отказаться от дачи показаний по делу своего клиента?
Какие госорганы имеют доступ к банковской тайне без согласия клиента?

Нормативно-правовые акты РФ

17. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
18. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
19. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
20. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

13. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)

14. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
15. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

13. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
14. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
15. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

13. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
14. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
15. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 6: Анализ аспектов обеспечения правовой защиты конфиденциальной информации

Цель работы:

1. Изучить правовые механизмы защиты конфиденциальной информации
2. Проанализировать нормативную базу РФ в области защиты информации
3. Разработать практические рекомендации по обеспечению информационной безопасности
4. Сформировать навыки анализа правовых рисков и разработки защитных мер

1. Теоретическая часть

1.1. Понятие и классификация конфиденциальной информации

Конфиденциальная информация - сведения, доступ к которым ограничен в соответствии с законодательством РФ. Классификация:

1. По виду тайны:
   - Государственная (Закон РФ № 5485-1)
   - Коммерческая (ФЗ № 98-ФЗ)
   - Персональные данные (ФЗ № 152-ФЗ)
   - Профессиональная (врачебная, адвокатская, нотариальная)

- Служебная (Указ Президента № 188)

2. По степени секретности:
- Особой важности
- Совершенно секретно
- Секретно
- Для служебного пользования

1.2. Нормативно-правовая база (детализированная таблица)

Уровень регулирования	Нормативный акт	Область применения
Международный	Конвенция Совета Европы № 108	Защита персональных данных
Федеральный	ФЗ № 149 "Об информации"	Общие положения
Отраслевой	Приказ ФСТЭК № 21	Требования к защите ПДн
Локальный	Положение о коммерческой тайне предприятия	Внутренний документооборот

1.3. Современные угрозы и вызовы

1. Киберугрозы:
- Фишинг атаки (+37% в 2023)
- Утечки через облачные сервисы
- Атаки на IoT-устройства

2. Правовые риски:
- Ужесточение штрафов за нарушения 152-ФЗ
- Расширение перечня КИИ (ФЗ № 187-ФЗ)
- Новые требования к трансграничной передаче данных

2. Практические задания

Задание 1. Комплексный анализ нормативной базы

Задача: Для выбранной организации (банк, мед.учреждение, IT-компания):

1. Составить таблицу применяемых нормативных актов
2. Провести анализ соответствия требованиям
3. Выявить потенциальные нарушения

Пример для медицинского центра:

Требование	Нормативный акт	Соответствие	Риски
Защита ПДн пациентов	ФЗ № 152-ФЗ ст. 19	Частичное (нет шифрования)	Штраф до 300 тыс. руб.
Хранение мед.карт	Приказ Минздрава № 29н	Полное	-
Использование облачных сервисов	Письмо Роскомнадзора № 08-187	Не соответствует	Блокировка сервиса

Задание 2. Глубокий разбор кейсов

Кейс 1. Утечка данных в банковском секторе
Ситуация: Несанкционированный доступ к базе данных 200,000 клиентов через уязвимость в API.
Этапы анализа:

1. Правовая квалификация:
   - Нарушение ст. 13.11 КоАП РФ
   - Возможное ст. 272 УК РФ
2. Технические причины:
   - Отсутствие WAF
   - Неактуальное ПО
3. Рекомендации:
   - Внедрение SIEM-системы
   - Регулярный аудит безопасности

Кейс 2. Конфликт коммерческих интересов
Ситуация: Бывший сотрудник передал конкурентам алгоритм ценообразования.
Правовой анализ:

1. Состав нарушения:
   - Неправомерное использование коммерческой тайны (ст. 183 УК РФ)
   - Нарушение трудового договора
2. Доказательная база:
   - Логи доступа
   - Электронная переписка
3. Меры защиты:
   - Система контроля доступа
   - Цифровые водяные знаки

Задание 3. Разработка системы защиты (практикум)
Этапы выполнения:

1. Анализ угроз:
   - Методология STRIDE
   - Оценка рисков по ГОСТ Р ИСО/МЭК 27005
2. Экономическое обоснование:
   - Расчет ROI на средства защиты
   - Сравнение стоимости внедрения и потенциальных убытков

3. Инструменты анализа

1. Правовые:
   - Системы "КонсультантПлюс", "Гарант"
   - Базы судебных решений
2. Технические:
   - OpenVAS для сканирования уязвимостей
   - Wireshark для анализа трафика
   - Metasploit для тестирования защиты
3. Методологические:
   - ГОСТ Р 57580.1-2017
   - NIST Cybersecurity Framework
   - Методики ФСТЭК России

Нормативно-правовые акты РФ

21. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
22. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
23. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
24. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

16. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
17. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
18. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

16. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
17. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
18. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

16. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
17. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
18. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 7: Правовое обеспечение защиты персональных данных

Цель работы: Изучить основные нормативно-правовые акты, регулирующие защиту персональных данных (ПДн), научиться анализировать требования законодательства и применять их на практике.

Задание 1. Теоретическая часть

1.1. Перечислите основные нормативно-правовые акты РФ, регулирующие обработку и защиту персональных данных. Укажите их ключевые положения.
1.2. Сравните ФЗ-152 "О персональных данных" и GDPR (General Data Protection Regulation) по следующим критериям:
Определение персональных данных
Принципы обработки
Права субъектов ПДн
Ответственность за нарушения
1.3. Какие организационные и технические меры защиты ПДн предусмотрены законодательством? Приведите примеры.

Задание 2. Практический кейс
Ситуация: Компания "DataSafe" занимается обработкой персональных данных клиентов (ФИО, паспортные данные, номера телефонов) для оказания услуг. В результате хакерской атаки произошла утечка данных 5000 клиентов.
Задания:
Какие статьи ФЗ-152 были нарушены?
Какие меры должна предпринять компания в соответствии с законодательством?
Какие виды ответственности (административная, уголовная, гражданско-правовая) могут наступить?
Разработайте рекомендации по предотвращению подобных инцидентов.

Задание 3. Разработка документации
Подготовьте "Политику обработки персональных данных" для условной организации (например, интернет-магазина). Включите разделы:
Цели обработки ПДн
Перечень обрабатываемых данных
Меры защиты (технические и организационные)
Права субъектов ПДн
Порядок реагирования на утечки

Нормативно-правовые акты РФ

25. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)

26. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)

27. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)

28. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

19. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)

20. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)

21. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

19. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)

20. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)

21. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

19. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
20. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
21. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 8: Правовая охрана и защита патентного и авторского права

Цель работы: Изучить основы патентного и авторского права, научиться анализировать случаи нарушений и применять правовые механизмы защиты интеллектуальной собственности в сфере IT и информационной безопасности.

Теоретическая часть

1. Основные понятия

1.1. Дайте определения:

Авторское право

Патентное право

Объекты авторского права (программы, базы данных, произведения)

Объекты патентного права (изобретения, полезные модели, промышленные образцы)

1.2. Перечислите основные нормативно-правовые акты РФ, регулирующие:

Авторское право (например, ГК РФ, часть 4)

Патентное право (ГК РФ, закон "О патентах")

Международные соглашения (Бернская конвенция, Соглашение ТРИПС)

1.3. Каковы сроки действия:

Авторского права

Патента на изобретение

Патента на полезную модель

Практическая часть

Задание 2. Анализ кейсов

Кейс 1. Нарушение авторских прав в IT

Компания "SoftDev" разработала уникальное ПО для защиты данных. Через 6 месяцев на рынке появился аналогичный продукт от компании "CopySoft" с идентичным кодом и интерфейсом.

Вопросы:

Какие права "SoftDev" нарушены?

Какие доказательства нужны для подачи иска?

Какие меры защиты можно применить (удаление контрафакта, компенсация)?

Какая ответственность предусмотрена по ст. 146 УК РФ?

Кейс 2. Патентный спор

Изобретатель создал новый алгоритм шифрования и подал заявку на патент. Через месяц другая компания выпустила продукт с аналогичным методом.

Вопросы:

Может ли изобретатель оспорить использование его алгоритма?

Каков порядок патентования программных решений в РФ?

Какие документы нужны для защиты патента?

Задание 3. Разработка документации

Ситуация: Ваша компания разрабатывает программное обеспечение. Необходимо обеспечить правовую защиту продукта.

Задание: Составьте "Положение о защите интеллектуальной собственности", включив:

Порядок регистрации авторских прав на ПО.

Алгоритм патентования изобретений.

Меры по предотвращению утечек исходного кода.

Действия при обнаружении нарушений (претензия, суд).

Нормативно-правовые акты РФ

29. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
30. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
31. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
32. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

22. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
23. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
24. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

22. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
23. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
24. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

22. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
23. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
24. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 9: Структура органов. Общие функции органов гос власти в области ИБ

Цель работы:
Изучить структуру и полномочия государственных органов, отвечающих за информационную безопасность в РФ, а также их роль в формировании и реализации политики ИБ.

Теоретическая часть
1. Основные государственные органы, регулирующие ИБ в РФ
1.1. Заполните таблицу:

Орган	Основные функции в сфере ИБ	Нормативные акты, регулирующие деятельность
Совет Безопасности РФ		
ФСБ России		
ФСТЭК России		
Минцифры России		
Роскомнадзор		

1.2. Дайте определение следующим терминам:
Национальная система защиты информации (НСЗИ)
Критическая информационная инфраструктура (КИИ)
Государственная тайна
Контроль соблюдения требований ИБ

Практическая часть
Задание 2. Анализ полномочий и взаимодействия органов
Ситуация: В результате кибератаки на банковскую систему произошла утечка данных клиентов и сбой в работе платежных систем.
Вопросы:
Какие государственные органы должны реагировать на инцидент?
Какие нормативные акты регулируют их действия?
Какие меры должны быть приняты для расследования и предотвращения подобных атак?
Как взаимодействуют между собой ФСБ, ФСТЭК и Роскомнадзор в подобных случаях?
Задание 3. Разработка схемы реагирования на киберинцидент
Задача: На основе изученных материалов разработайте "Алгоритм действий государственных органов при кибератаке на объект КИИ", включив:
Этапы выявления и оценки угрозы.
Распределение ролей между органами власти.
Меры по ликвидации последствий.

Профилактические меры для предотвращения повторных атак.

Нормативно-правовые акты РФ

1. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
2. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
3. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
4. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

1. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
2. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
3. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

1. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
2. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
3. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

1. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
2. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
3. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 10: Интеллектуальная собственность и патенты в сфере информационной безопасности

Цель работы: Изучить основы правовой охраны интеллектуальной собственности (ИС), особенности патентования IT-решений и алгоритмов, а также научиться применять полученные знания для защиты разработок в сфере информационной безопасности.

Теоретическая часть

1. Основные понятия интеллектуальной собственности

1.1. Дайте определение следующим терминам:

Интеллектуальная собственность (ИС)

Авторское право

Патентное право

Промышленный образец

Товарный знак

1.2. Какие объекты ИС наиболее актуальны в сфере информационной безопасности? Приведите примеры (например, алгоритмы шифрования, ПО, базы данных).

1.3. Перечислите основные нормативные акты, регулирующие ИС в РФ:

Часть IV Гражданского кодекса РФ

Закон «О патентах»

Международные соглашения (Бернская конвенция, Соглашение ТРИПС)

Практическая часть

Задание 2. Анализ кейсов

Кейс 1. Патентование алгоритма шифрования

Компания «CryptoGuard» разработала новый метод асимметричного шифрования и хочет его запатентовать.

Вопросы:

Можно ли запатентовать алгоритм в РФ? Какие условия должны быть соблюдены?

Какие этапы патентования необходимо пройти?

Какие документы потребуются для подачи заявки в Роспатент?

Каков срок действия патента на изобретение?

Кейс 2. Нарушение авторских прав на ПО

Студент разработал программу для анализа уязвимостей и выложил её в открытый доступ под лицензией GPL. Через полгода коммерческая компания начала продавать этот продукт без указания авторства.

Вопросы:

Какие права студента нарушены?

Какие действия он может предпринять для защиты своих прав?

Какие виды ответственности (гражданская, административная, уголовная) могут быть применены к нарушителю?

Задание 3. Разработка патентной заявки

Ситуация: Вы разработали новый метод обнаружения вторжений в сеть (IDS). Необходимо подготовить заявку на патент.
Задание: Составьте «Описание изобретения», включающее:
Название и область применения.
Техническую задачу, которую решает изобретение.
Сущность изобретения (принцип работы).
Пример реализации (схемы, формулы, если требуется).

Нормативно-правовые акты РФ

1. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
2. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
3. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
4. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

1. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
2. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
3. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

1. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
2. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
3. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

1. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
2. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
3. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:

Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 11: Министерство обороны РФ и ФСТЭК России в системе информационной безопасности

Цель работы: Изучить структуру, функции и полномочия Министерства обороны РФ и Федеральной службы по техническому и экспортному контролю (ФСТЭК России) в сфере обеспечения информационной безопасности (ИБ), а также их роль в защите государственных информационных ресурсов.

Теоретическая часть
1. Министерство обороны РФ в системе ИБ
1.1. Основные функции Минобороны России в сфере ИБ:
Защита информации в Вооружённых Силах РФ
Обеспечение безопасности систем управления войсками
Противодействие киберугрозам в оборонной сфере
Участие в разработке политики ИБ государства
1.2. Нормативные документы, регулирующие деятельность Минобороны в ИБ:
Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации»
Доктрина информационной безопасности РФ
Ведомственные акты Минобороны
1.3. Структурные подразделения Минобороны, отвечающие за ИБ:
Главное управление Генштаба ВС РФ (ГУ ГШ ВС РФ)
Центр информационной безопасности Минобороны
2. ФСТЭК России и её роль в ИБ
2.1. Основные функции ФСТЭК:
Контроль защиты информации в госорганах и КИИ (критической информационной инфраструктуре)
Лицензирование деятельности по технической защите информации
Сертификация средств защиты информации
Противодействие техническим разведкам
2.2. Нормативные акты, регулирующие деятельность ФСТЭК:
Федеральный закон №187-ФЗ «О безопасности КИИ»
Постановления ФСТЭК (например, №17 «О требованиях к защите информации»)
Приказы ФСТЭК по сертификации СЗИ
2.3. Ключевые направления работы ФСТЭК:
Аттестация объектов информатизации
Контроль выполнения требований по ИБ
Разработка методик защиты информации

Практическая часть

Задание 3. Сравнительный анализ Минобороны и ФСТЭК
Заполните таблицу:

Критерий	Минобороны РФ	ФСТЭК России
Основная сфера деятельности		
Объекты защиты		
Нормативные акты		
Методы контроля и защиты		

Задание 4. Кейс-анализ
Ситуация: Хакерская группа атаковала информационные системы оборонного предприятия. Часть данных попала в открытый доступ.
Вопросы:

1. Какие структуры (Минобороны/ФСТЭК) должны участвовать в расследовании?
2. Какие нормативные акты регулируют их действия?
3. Какие меры должны быть приняты для устранения последствий?
4. Как организовано взаимодействие между Минобороны и ФСТЭК в подобных случаях?

Нормативно-правовые акты РФ

1. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
2. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
3. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
4. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

1. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
2. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
3. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

1. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
2. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
3. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

1. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
2. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
3. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 12: Лицензирование и сертификация в области информационной безопасности

Цель работы: Изучить нормативно-правовую базу, процедуры и особенности лицензирования деятельности и сертификации средств защиты информации в Российской Федерации.

Теоретическая часть

1. Лицензирование деятельности в области ИБ
1.1. Основные понятия:
Лицензия ФСТЭК и ФСБ
Лицензируемые виды деятельности (по 99-ФЗ и 187-ФЗ)
Требования к соискателям лицензии
1.2. Нормативная база:
Федеральный закон №99-ФЗ «О лицензировании отдельных видов деятельности»
Постановление Правительства №313 «О лицензировании деятельности по ТЗКИ»
Приказы ФСТЭК №17, №21
1.3. Процедура получения лицензии:
Подготовка документов
Подача заявления
Проверка соответствия требованиям
Выдача лицензии

2. Сертификация средств защиты информации (СЗИ)
2.1. Основные понятия:
Обязательная и добровольная сертификация
Сертификат соответствия ФСТЭК/ФСБ
Реестр сертифицированных СЗИ
2.2. Нормативная база:
Федеральный закон №184-ФЗ «О техническом регулировании»
Приказы ФСТЭК №76, №239
Требования защиты информации (СПД, ГИС, КИИ)
2.3. Этапы сертификации:
Подача заявки
Лабораторные испытания
Анализ результатов
Выдача сертификата

Практическая часть
Задание 3. Сравнительный анализ
Заполните таблицу:

Критерий	Лицензирование	Сертификация
Регулирующий орган		
Нормативные акты		
Срок действия		
Ответственность за нарушение		

Задание 4. Кейс-анализ
Ситуация 1: Компания «ЗащитаИнфо» оказывает услуги по технической защите информации, но не имеет лицензии ФСТЭК.
Вопросы:
- Какие нарушения допустила компания?
- Какие санкции могут быть применены?
- Какие шаги необходимо предпринять для легализации деятельности?

Ситуация 2: При проверке банка выявлено использование несертифицированного межсетевого экрана в системе обработки персональных данных.
Вопросы:
- Какие требования нарушены?
- Кто несет ответственность?
- Какие меры необходимо принять?

Нормативно-правовые акты РФ
1. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)

2. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
3. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
4. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

1. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
2. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
3. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

1. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
2. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
3. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

1. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
2. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
3. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

8 семестр

Практическая работа 13: Уголовная ответственность в сфере ИБ

Цель работы: Изучить состав преступлений в сфере информационной безопасности, предусмотренных Уголовным кодексом РФ, и научиться анализировать практические случаи киберпреступлений.

Теоретическая часть

1. Основные статьи УК РФ в сфере ИБ

1.1. Заполните таблицу:

Статья УК РФ	Состав преступления	Максимальное наказание
Статья 272 (Неправомерный доступ к компьютерной информации)		
Статья 273 (Создание, использование и распространение вредоносных программ)		
Статья 274 (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации)		
Статья 274.1 (Неправомерное воздействие на критическую информационную инфраструктуру)		
Статья 159.6 (Мошенничество в сфере компьютерной информации)		

1.2. Дайте определение следующим терминам:

Компьютерная информация

Вредоносная программа

Критическая информационная инфраструктура

Неправомерный доступ

Практическая часть

Задание 2. Анализ кейсов

Кейс 1: Сотрудник IT-отдела банка, имея доступ к базе данных, скопировал и продал персональные данные клиентов.

Вопросы:

- Какая статья УК РФ нарушена?
- Какие отягчающие обстоятельства могут быть?
- Какие технические меры могли бы предотвратить преступление?

Кейс 2: Злоумышленник создал и распространил вирус-шифровальщик, который заблокировал работу городской больницы.

Вопросы:

- Какие статьи УК РФ применимы?
- Какова может быть мера наказания?
- Какие технические следы могут помочь в расследовании?

Задание 3. Разработка мер профилактики

Ситуация: В компании произошла утечка данных из-за действий сотрудника.
Задание: Разработайте "Памятку по предотвращению внутренних угроз ИБ", включив: Меры контроля доступа, Системы мониторинга действий сотрудников, Порядок реагирования на инциденты, Обучение сотрудников

Нормативно-правовые акты РФ

1. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
2. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
3. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
4. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

1. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
2. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
3. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

1. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
2. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
3. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

1. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
2. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
3. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России

Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 14: Основы работы с российскими и международными стандартами в области информационной безопасности

Цель работы: Изучить ключевые российские и международные стандарты в области информационной безопасности, научиться анализировать их требования и применять на практике для защиты информационных систем.

Теоретическая часть

1. Российские стандарты ИБ

1.1. Заполните таблицу:

Стандарт	Область применения	Ключевые требования
ГОСТ Р 57580.1-2017 (Безопасность финансовых организаций)		
ГОСТ Р ИСО/МЭК 27001-2022 (Менеджмент информационной безопасности)		
ГОСТ Р 56939-2016 (Защита персональных данных)		
СП 50-149-2021 (Требования к защите информации в КИИ)		

1.2. Дайте определение: Государственный стандарт (ГОСТ), Свод правил (СП), Технический регламент

2. Международные стандарты ИБ

2.1. Заполните таблицу:

Стандарт	Страна/Организация	Область применения
ISO/IEC 27001	ISO/IEC	
NIST SP 800-53	США	
PCI DSS	PCI SSC	
GDPR	ЕС	

2.2. Сравните ГОСТ Р ИСО/МЭК 27001 и ISO/IEC 27001:

- Область применения
- Структура документа
- Процесс сертификации

Практическая часть

Задание 3. Анализ стандартов

Кейс 1: Компания разрабатывает систему обработки персональных данных для банка.

Задание:

- Какие российские стандарты необходимо учитывать?
- Какие разделы ГОСТ Р 56939-2016 наиболее важны?
- Какой международный стандарт можно использовать дополнительно?

Кейс 2: Производитель программного обеспечения хочет получить сертификат соответствия ISO 27001.

Задание:

- Опишите этапы подготовки к сертификации
- Какие документы необходимо разработать?
- Какой российский стандарт является аналогом?

Нормативно-правовые акты РФ

1. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
2. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
3. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
4. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

1. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
2. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
3. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

1. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
2. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)

3. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

1. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
2. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
3. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 15: Анализ стандартов информационной безопасности

Цель работы: Научиться анализировать, сравнивать и применять российские и международные стандарты информационной безопасности на практике.

Теоретическая часть

1. Классификация стандартов ИБ

1.1. Заполните таблицу, указав тип стандарта и область применения:

Стандарт	Тип (международный/российский)	Область применения
ISO/IEC 27001		
ГОСТ Р 57580.1-2017		
PCI DSS v4.0		
NIST Cybersecurity Framework		
ГОСТ Р ИСО/МЭК 15408		

1.2. Ответьте на вопросы:

- Чем отличаются обязательные и рекомендательные стандарты?
- Какие организации разрабатывают стандарты ИБ в России и мире?
- Как стандарты ИБ связаны с законодательством?

Практическая часть

Задание 2. Сравнительный анализ стандартов

Задача: Сравните два стандарта по следующим критериям:

Критерий	Стандарт 1 (укажите какой)	Стандарт 2 (укажите какой)
Год принятия		
Разработчик		
Область применения		
Структура документа		
Процесс внедрения		
Сертификация		

Рекомендуемые пары для анализа:
ISO 27001 vs ГОСТ Р ИСО/МЭК 27001
PCI DSS vs ГОСТ Р 57580.1-2017
NIST CSF vs ГОСТ Р 59582-2021

Задание 3. Кейс-анализ
Кейс 1: Банк планирует внедрить систему защиты персональных данных.
Задание:

- Какие стандарты необходимо учитывать?
- Составьте таблицу соответствия требований ГОСТ Р 56939 и ISO 27001
- Предложите поэтапный план внедрения

Кейс 2: IT-компания разрабатывает облачное решение для госсектора.
Задание:

- Какие стандарты безопасности обязательны для соблюдения?
- Как провести оценку соответствия требованиям?
- Разработайте чек-лист для аудита

Задание 4. Разработка фрагмента документации
Ситуация: Для компании требуется разработать политику управления доступом.
Задание: На основе стандарта ISO 27002:

- Составьте перечень обязательных разделов
- Разработайте 3-4 конкретных требования к управлению учетными записями
- Предложите механизмы контроля выполнения

Нормативно-правовые акты РФ

1. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
2. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
3. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)

4. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

1. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
2. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
3. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

1. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
2. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
3. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

1. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
2. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
3. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 16: Анализ структуры и нормативной базы компании

Цель работы: Научиться анализировать организационную структуру компании и ее нормативную базу с точки зрения обеспечения информационной безопасности, выявлять слабые места и разрабатывать рекомендации по улучшению.

Теоретическая часть

1. Основные элементы структуры компании в контексте ИБ

1.1. Заполните таблицу:

Элемент структуры	Роль в обеспечении ИБ	Пример подразделения/должности
Руководство компании		
IT-отдел		
Отдел информационной безопасности		
Обычные сотрудники		

1.2. Ответьте на вопросы:

- Почему важно учитывать организационную структуру при построении системы ИБ?
- Как распределяются роли и ответственность за ИБ в компании?
- Какие документы регулируют работу подразделений в области ИБ?

2. Нормативная база компании по ИБ

2.1. Перечислите основные виды внутренних документов по ИБ:

- Политики
- Регламенты
- Инструкции
- Процедуры

2.2. Заполните таблицу, указав назначение каждого документа:

Тип документа	Назначение	Пример
Политика информационной безопасности		
Регламент доступа к информации		
Инструкция по работе с персональными данными		
Процедура реагирования на инциденты		

Практическая часть

Задание 3. Анализ структуры компании

Кейс: Компания "ТехноПро" (150 сотрудников, занимается разработкой ПО) имеет следующую структуру:

- Руководство
- IT-отдел (5 человек)
- Отдел разработки (50 человек)
- Отдел продаж (20 человек)
- Бухгалтерия (5 человек)
- Отдел кадров (3 человека)

Задание:

- Выявите риски ИБ для каждой группы сотрудников
- Определите, каких подразделений не хватает для обеспечения ИБ

- Предложите изменения в структуре

Задание 4. Анализ нормативной базы
Ситуация: В компании есть только: Положение о коммерческой тайне; Инструкция по работе с электронной почтой
Задание:
- Составьте перечень недостающих документов
- Разработайте структуру Политики ИБ
- Напишите фрагмент регламента доступа (3-4 пункта)

Задание 5. Разработка рекомендаций
На основе проведенного анализа:
Составьте план внедрения изменений (этапы, сроки, ответственные)
Разработайте чек-лист для аудита нормативной базы
Предложите программу обучения сотрудников

Нормативно-правовые акты РФ

1. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
2. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
3. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
4. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

1. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
2. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
3. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

1. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
2. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)

3. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

1. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
2. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
3. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 17: Разработка политики безопасности компании

Цель работы: Разработать комплексную политику информационной безопасности для конкретной организации с учетом отраслевых особенностей и нормативных требований.

1. Подготовительный этап

1.1. Анализ объекта защиты

Задание: Выберите организацию (реальную или гипотетическую) и опишите:

- Сферу деятельности
- Количество сотрудников
- Особенности информационной инфраструктуры
- Основные информационные активы

Форма представления: Таблица с характеристиками компании

1.2. Нормативный анализ

Задание: Для выбранной организации определите:

- 3 обязательных нормативных документа (ГОСТ, ФЗ)
- 2 рекомендуемых международных стандарта
- Отраслевые требования (при наличии)

2. Проектирование политики

2.1. Разработка структуры

- Базовые разделы:
- Общие положения
- Зоны ответственности
- Классификация данных
- Управление доступом
- Защита конфиденциальной информации

- Реагирование на инциденты
- Контроль и аудит

Задание: Дополните структуру 2-3 специализированными разделами, актуальными для выбранной организации

2.2. Детализация разделов

Пример задания: Для раздела "Управление доступом" разработайте:

- 3 уровня доступа к информации
- Правила создания и блокировки учетных записей
- Требования к парольной политике
- Процедуру предоставления временного доступа

3. Практическая реализация

3.1. План внедрения

- Разработайте поэтапный план на 3 месяца:
- Подготовительный этап (аудит, обучение)
- Пилотное внедрение (выбор подразделения)
- Полномасштабное внедрение

3.2. Инструменты контроля

Создайте:

- Чек-лист проверки соблюдения политики
- Форму отчета о нарушениях
- Анкету для оценки осведомленности сотрудников

Нормативно-правовые акты РФ

1. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
2. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
3. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
4. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

1. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
2. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
3. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

1. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
2. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
3. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

1. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
2. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
3. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 18: Разработка модели угроз компании

Цель работы: Научиться анализировать информационные активы компании, выявлять угрозы и разрабатывать модель угроз в соответствии с международными и российскими стандартами.

1. Теоретическая часть

1.1. Основные понятия
Задание: Дайте определения следующим терминам:

- Модель угроз
- Уязвимость
- Риск информационной безопасности
- Актив (актив компании)
- Вопросы для обсуждения:
- Почему модель угроз — это основа для построения системы защиты информации?
- Какие стандарты (ГОСТ, ISO, NIST) регламентируют разработку модели угроз?

1.2. Классификация угроз
Задание: Заполните таблицу, указав примеры угроз для каждого типа:

Тип угрозы	Источник угрозы	Пример
Внешние кибератаки	Хакеры, конкуренты	Фишинг, DDoS-атаки
Внутренние угрозы	Сотрудники, подрядчики	Утечка данных, саботаж
Технические сбои	Оборудование, ПО	Отказ сервера, ошибки в коде
Природные и техногенные	Стихийные бедствия	Пожар, наводнение

2. Практическая часть

2.1. Анализ компании

Кейс: Компания "БанкСейф" (средний банк, 500 сотрудников):

- Онлайн-банкинг и мобильное приложение
- База данных клиентов (ПДн)
- Облачное хранилище документов
- Удаленные сотрудники

Задание:

- Определите 5 ключевых активов, которые нужно защищать.
- Выявите 3 наиболее опасных угрозы для каждого актива.
- Оцените вероятность (низкая/средняя/высокая) и возможный ущерб (1-5 баллов).

2.2. Разработка модели угроз

Структура модели:

- Цель модели (защита каких активов?)
- Активы компании (серверы, базы данных, сотрудники)
- Угрозы (список + источники)
- Уязвимости (слабые места в защите)
- Риски (вероятность × ущерб)
- Рекомендации по защите

Задание: Разработайте модель угроз для "БанкСейф", заполнив таблицу:

Актив	Угроза	Уязвимость	Риск (вероятность/ущерб)	Меры защиты
База данных клиентов	Утечка через сотрудника	Слабый контроль доступа	Высокий/5	Двухфакторная аутентификация

2.3. Оценка рисков и рекомендации

Задание: Постройте матрицу рисков (вероятность vs ущерб).

- Выделите 3 критических риска, требующих немедленного устранения.
- Предложите конкретные меры защиты (технические, организационные).

Нормативно-правовые акты РФ

1. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
2. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
3. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
4. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

1. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
2. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
3. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

1. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
2. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
3. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

1. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
2. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
3. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 19: Разработка модели нарушителя

Цель работы: Научиться анализировать и классифицировать потенциальных нарушителей информационной безопасности, разрабатывать профили нарушителей и применять полученные знания для построения эффективной системы защиты информации.

1. Теоретическая часть

1.1. Основные понятия

Задание: Дайте определения следующим терминам:

- Модель нарушителя
- Классификация нарушителей
- Мотивы нарушителей
- Потенциальный ущерб
- Вопросы для обсуждения:
- Почему важно учитывать модель нарушителя при построении системы защиты информации?
- Какие стандарты (ГОСТ, ISO, NIST) регламентируют разработку модели нарушителя?

1.2. Классификация нарушителей

Задание: Заполните таблицу, указав характеристики для каждого типа нарушителя:

Тип нарушителя	Уровень доступа	Мотивы	Методы атак
Внешний злоумышленник	Нет доступа	Финансовая выгода, хактивизм	Фишинг, DDoS, эксплуатация уязвимостей
Внутренний нарушитель	Ограниченный/полный	Месть, корысть, неосторожность	Кража данных, саботаж
Инсайдер	Полный доступ	Шпионаж, конкурентная борьба	Утечка информации, backdoor
Случайный нарушитель	Ограниченный	Любопытство, ошибки	Непреднамеренные действия

---

2. Практическая часть

2.1. Анализ компании

Кейс: Компания "ТехноПро" (разработка ПО, 150 сотрудников):

- Разрабатывает программное обеспечение для банков
- Имеет доступ к финансовым данным клиентов
- Использует облачные сервисы и удалённую работу

Задание: Определите 3 ключевых актива, которые могут быть целью нарушителей.

- Выявите 3 наиболее вероятных типа нарушителей для данной компании.
- Оцените уровень угрозы (низкий/средний/высокий) и потенциальный ущерб (1-5 баллов).

2.2. Разработка модели нарушителя
Структура модели:

- Профиль нарушителя (роль, доступ, навыки)
- Мотивы и цели
- Методы атак
- Способы противодействия

Задание: Разработайте модель нарушителя для "ТехноПро", заполнив таблицу:

Тип нарушителя	Профиль	Мотивы	Методы атак	Защитные меры
Внешний хакер	Опытный, использует эксплойты	Финансовая выгода	Атаки на API, фишинг	WAF, обучение сотрудников

2.3. Оценка рисков и рекомендации
Задание:
Постройте матрицу рисков (вероятность × ущерб).
Выделите 2 наиболее опасных нарушителя.
Предложите конкретные меры защиты (технические, организационные).

Нормативно-правовые акты РФ

1. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
2. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
3. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
4. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

1. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
2. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)

3. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

1. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
2. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
3. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

1. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
2. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
3. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 20: Организация службы безопасности компании

Цель работы: Сформировать практические навыки проектирования организационной структуры и регламентов работы службы информационной безопасности (СИБ) компании с учетом отраслевых требований и международных стандартов.

1. Теоретический раздел

1.1. Основные модели организации СИБ
Задание: Сравните три модели:

- Централизованная
- Децентрализованная
- Гибридная

Критерий	Централизованная	Децентрализованная	Гибридная
Уровень контроля			
Гибкость			
Стоимость			

1.2. Нормативная база
Задание: Укажите, какие требования предъявляют:

- ФЗ-152 "О персональных данных"
- ФЗ-187 "О КИИ"
- ГОСТ Р ИСО/МЭК 27001

2. Практический раздел

2.1. Проектирование структуры СИБ

Кейс: Компания "ТехноГарант" (400 сотрудников):

Разработка ПО для госсектора

Обработка ПДн 100,000+ клиентов

5 филиалов в разных регионах

Задание:

- Разработайте оптимальную структуру СИБ (схема + пояснения)
- Распределите функции между:
- Руководителем СИБ
- Аналитиками рисков
- Специалистами по реагированию

2.2. Регламентирующие документы

Задание: Составьте:

- Положение о СИБ (основные разделы)
- Должностную инструкцию специалиста ИБ
- Регламент взаимодействия с IT-отделом

Нормативно-правовые акты РФ

1. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
2. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
3. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
4. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

1. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
2. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
3. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

1. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
2. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
3. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

1. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
2. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
3. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 21: Организация внутриобъектного режима компании

Цель работы: Освоить принципы организации внутриобъектового режима на предприятии, разработать комплекс мер по обеспечению физической и информационной безопасности с учетом нормативных требований.

1. Теоретическая часть

1.1. Основные понятия
Задание: Дайте определения:

- Внутриобъектовый режим
- Пропускной режим
- Контрольная зона
- Объектовая охрана

Вопросы:

- Чем отличается внутриобъектовый режим от пропускного?
- Какие нормативные документы регулируют организацию режима на предприятии?

1.2. Нормативная база
Задание: Заполните таблицу:

Нормативный документ	Требования к организации режима
ФЗ-149 "Об информации"	

Нормативный документ	Требования к организации режима
Постановление Правительства №1119	
ГОСТ Р 57580.1-2017	

2. Практическая часть

2.1. Анализ объекта

Кейс: Офис IT-компании "КодБезопасности" (3 этажа, 120 сотрудников):
Разработка ПО для госзаказчиков
Серверная комната на 2 этаже
Архив документации
Задание:

- Выделите 3 ключевые зоны с разным уровнем доступа
- Определите 5 потенциальных угроз безопасности
- Составьте таблицу контроля доступа

2.2. Разработка режимных мероприятий

Разделы для разработки:

- Пропускная система:
- Типы пропусков (постоянные, временные, разовые)
- Порядок учета и выдачи
- Зонирование территории:
- Общая зона
- Зона ограниченного доступа
- Режимная зона
- Контроль посетителей:
- Журнал учета
- Сопровождение

Задание: Разработайте: Инструкцию дежурного по пропускному пункту

- Схему зонирования офиса
- Регламент экстренной эвакуации

2.3. Технические средства защиты

Задание: Подберите оборудование для:

- Контроля доступа (СКУД)
- Видеонаблюдения
- Охраны периметра

Зона	Технические средства	Обоснование выбора
Входная группа		
Серверная		
Архив		

Нормативно-правовые акты РФ

1. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
2. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
3. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
4. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

1. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
2. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
3. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

1. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
2. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
3. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

1. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
2. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
3. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 22: Организация видеонаблюдения компании

Цель работы: Освоить принципы проектирования, развертывания и администрирования систем видеонаблюдения с учетом требований информационной безопасности.

1. Теоретическая часть

1.1. Основные понятия

Задание: Дайте определения:

- CCTV (Closed-Circuit Television)
- IP-видеонаблюдение
- Глубина архива видеозаписей
- Детекция движения

Вопросы:

- Чем отличается аналоговое видеонаблюдение от IP-систем?
- Какие нормативные документы регулируют использование видеонаблюдения?

1.2. Нормативная база

Задание: Заполните таблицу:

Нормативный документ	Требования к видеонаблюдению
ФЗ-152 "О персональных данных"	
ГОСТ Р 51558-2014	
Постановление №1119	

2. Практическая часть

2.1. Проектирование системы

Кейс: Офис компании "DataSecure" (2 этажа, 800 м²):

- 3 входа/выхода
- Серверная комната
- Зона reception
- Открытый офис (50 рабочих мест)

Задание: Разработайте схему размещения камер (планировка + пояснения)

Рассчитайте необходимое количество камер по формуле:

Copy

$N = S / (k \times D^2)$, где:

S - площадь зоны

k - коэффициент (0.5-0.7)

D - дальность детализации

Выберите тип камер для разных зон

Зона	Тип камеры	Характеристики	Обоснование
Входная группа	Купольная IP 4Мп	IR-подсветка 30м	Контроль лиц

2.2. Выбор оборудования
Задание: Сравните 3 варианта комплектации:

Компонент	Бюджетный	Оптимальный	Премиум
Камеры			
Видеорегистратор			
Хранилище			
ПО			

2.3. Интеграция с ИБ
Задание: Разработайте:

- Регламент доступа к архиву
- Меры защиты видеопотока (шифрование, VLAN)
- Политику хранения записей

Нормативно-правовые акты РФ

1. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
2. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
3. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
4. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

1. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
2. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
3. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

1. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
2. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
3. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

1. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
2. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
3. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 23: Организация пропускного режима

Цель работы: Освоить принципы проектирования и внедрения эффективного пропускного режима, обеспечивающего контроль доступа персонала и посетителей с учетом требований информационной безопасности.

1. Теоретическая часть

1.1. Основные понятия
Задание: Дайте определения:

- Пропускной режим
- СКУД (система контроля и управления доступом)
- Биометрическая идентификация
- Зонирование территории
- Вопросы:
- Какие задачи решает пропускной режим в контексте ИБ?
- Чем отличается физический контроль доступа от логического?

1.2. Нормативная база
Задание: Заполните таблицу:

Нормативный документ	Требования к пропускному режиму
ФЗ-149 "Об информации"	
Постановление Правительства №1119	

Нормативный документ	Требования к пропускному режиму
ГОСТ Р 51241-2008 (СКУД)	

2. Практическая часть

2.1. Анализ объекта

Кейс: Офис IT-компании "CyberShield" (3 этажа, 200 сотрудников):
2 входа (центральный и служебный)
Серверная комната (3-й этаж)
Архив документации
Парковка для сотрудников
Задание:

- Разделите территорию на зоны доступа (схема + пояснения)
- Определите категории персонала и их права доступа
- Выявите 3 наиболее уязвимых места

2.2. Проектирование системы

Разделы для разработки:

- Типы пропусков:
- Постоянные (сотрудники)
- Временные (подрядчики)
- Разовые (посетители)
- Идентификация:
- Пластиковые карты
- Биометрия (отпечатки пальцев)
- Мобильные пропуска
- Технические средства:
- Турникеты/шлюзы
- Считыватели
- ПО для учета

Задание:

- Разработайте схему размещения СКУД
- Составьте таблицу прав доступа

Категория	Доступные зоны	Тип идентификации
Сотрудник	Все зоны, кроме серверной	Карта + PIN

2.3. Регламентирующие документы

Задание: Разработайте:

- Инструкцию для охраны (порядок проверки пропусков)
- Положение о пропускном режиме (основные разделы)
- Журнал учета посетителей (образец)

Нормативно-правовые акты РФ

1. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
2. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
3. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
4. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

1. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
2. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
3. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

1. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
2. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
3. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

1. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
2. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
3. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 24: Аудит информационной безопасности

Цель работы: Освоить методику проведения аудита информационной безопасности, научиться выявлять уязвимости и разрабатывать рекомендации по улучшению защиты информации.

1. Теоретическая часть

1.1. Основные понятия

Задание: Дайте определения:

- Аудит ИБ
- Уязвимость
- Риск
- Комплаенс-проверка
- Вопросы:
- Чем отличается внутренний аудит от внешнего?
- Какие стандарты регламентируют проведение аудита ИБ?

1.2. Нормативная база

Задание: Заполните таблицу:

Стандарт/Регламент	Область применения
ГОСТ Р ИСО/МЭК 27001	
PCI DSS v4.0	
ФСТЭК Приказ №17	

2. Практическая часть

2.1. Подготовка к аудиту

Кейс: Компания "DataSecure" (разработка ПО, 150 сотрудников):

Использует облачные сервисы

Обрабатывает персональные данные

Имеет удаленных сотрудников

Задание:

- Определите 3 ключевых актива для проверки
- Составьте чек-лист на основе ГОСТ Р ИСО/МЭК 27001 (10 пунктов)
- Выберите методы аудита (интервью, сканирование, анализ документов)

2.2. Проведение аудита

Этапы проверки:

- Анализ документов (политики, регламенты)
- Техническая проверка (сканирование сети, тест на проникновение)
- Опрос сотрудников (уровень осведомленности)
- Задание:
- Проведите аудит парольной политики (на основе чек-листа)
- Выявите 3 уязвимости в системе доступа
- Оцените риски по матрице (вероятность × ущерб)

Уязвимость	Уровень риска	Рекомендации
Слабые пароли	Высокий	Внедрить 2FA

2.3. Отчет по аудиту
Структура отчета:
- Введение (цель, методы)
- Результаты (найденные уязвимости)
- Рекомендации (сроки, ответственные)

Задание: Подготовьте фрагмент отчета по одному из выявленных нарушений (2-3 страницы)

Нормативно-правовые акты РФ

1. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
2. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
3. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
4. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

1. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
2. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
3. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

1. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
2. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
3. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

1. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
2. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
3. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 25: Лицензирование деятельности в области защиты информации

Цель работы: Изучить нормативно-правовую базу лицензирования деятельности в сфере защиты информации, ознакомиться с требованиями к получению лицензий ФСТЭК и ФСБ России, а также проанализировать практические аспекты лицензирования.

Теоретическая часть

1. Основные нормативные документы
   - Перечислите и кратко охарактеризуйте ключевые нормативные акты, регулирующие лицензирование деятельности в области защиты информации:
   - Федеральный закон № 99-ФЗ "О лицензировании отдельных видов деятельности"
   - Федеральный закон № 149-ФЗ "Об информации, информационных технологиях и о защите информации"
   - Постановления Правительства РФ, регулирующие лицензирование в сфере защиты информации (например, № 171, № 313)
   - Приказы ФСТЭК России и ФСБ России, устанавливающие требования к лицензиатам
2. Виды лицензируемой деятельности
   - Укажите, какие виды деятельности подлежат лицензированию в сфере защиты информации (например):
   - Разработка и производство средств защиты информации (СЗИ)
   - Техническая защита конфиденциальной информации (ТЗКИ)
   - Деятельность по выявлению электронных устройств перехвата информации (ПДУ)
   - Противодействие иностранным техническим разведкам (ПДТР)
3. Требования к соискателям лицензии
   - Опишите основные требования к организациям, претендующим на получение лицензии:
   - Наличие квалифицированных специалистов (с аттестатами ФСТЭК/ФСБ)
   - Наличие защищённых помещений (для работы с гостайной)

- Использование сертифицированных средств защиты информации
- Наличие системы менеджмента безопасности информации (СМБИ)

Практическая часть

Задание 1. Анализ лицензионных требований

Найдите на официальных сайтах ФСТЭК (fstec.ru) и ФСБ (fsb.ru) актуальные требования к лицензированию.

Сравните условия лицензирования для двух видов деятельности (например, ТЗКИ и разработка СЗИ).

Составьте таблицу с основными различиями.

Критерий	ТЗКИ (ФСТЭК)	Разработка СЗИ (ФСБ)
Необходимые документы		
Требования к персоналу		
Сертификация СЗИ		

Задание 2. Разбор кейса

Ситуация: Компания "КиберЗащита" хочет получить лицензию ФСТЭК на техническую защиту конфиденциальной информации. В штате есть 3 специалиста с аттестатами, но отсутствует сертифицированное ПО для защиты данных.

Вопросы:

- Какие шаги должна предпринять компания для получения лицензии?
- Какие проблемы могут возникнуть при проверке?
- Какие нормативные документы будут проверяться?

Задание 3. Ситуационная задача

Представьте, что вы – сотрудник отдела информационной безопасности компании. Руководство планирует начать работу с государственными заказчиками, но у организации нет лицензии ФСБ.

Задача: Составьте пошаговый план действий для получения необходимой лицензии, указав:

- Какие виды лицензий нужны?
- Какие документы необходимо подготовить?
- Сколько времени займёт процесс?

Нормативно-правовые акты РФ

1. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
2. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
3. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)

4. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

1. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
2. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)
3. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

1. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
2. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
3. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

1. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
2. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
3. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)

Практическая работа 26: Анализ требований ГОСТ Р 56939-2024

Цель работы: Изучить требования стандарта ГОСТ Р 56939-2024 «Защита информации. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных», проанализировать его ключевые положения и применить их в практических кейсах.

Теоретическая часть

1. Общая характеристика ГОСТ Р 56939-2024

Область применения: Обеспечение безопасности персональных данных (ПДн) в информационных системах (ИСПДн).
Соответствие законодательству: Соответствует требованиям ФЗ-152 "О персональных данных" и приказам ФСТЭК России.
Основные термины:
ИСПДн – информационная система персональных данных.
Угрозы безопасности ПДн – потенциальные воздействия на данные, приводящие к утечке или модификации.
Меры защиты – организационные и технические способы защиты ПДн.
2. Ключевые требования стандарта
2.1. Классификация ИСПДн
Категории систем (по уровню угроз):
1-й уровень (высокая угроза) – биометрические, специальные ПДн.
2-й уровень (средняя угроза) – массовые ПДн (сотрудники, клиенты).
3-й уровень (низкая угроза) – обезличенные или публичные данные.
2.2. Меры защиты ПДн
Организационные меры:

- Назначение ответственного за защиту ПДн.
- Разработка политики безопасности.
- Обучение сотрудников.
- Технические меры:
- Использование СКЗИ (средств криптографической защиты информации).
- Контроль доступа (аутентификация, авторизация).
- Защита от вредоносного ПО.
- Резервное копирование и восстановление данных.

2.3. Требования к инфраструктуре

- Физическая защита:
- Ограничение доступа в серверные помещения.
- Видеонаблюдение, системы контроля доступа (СКУД).
- Сетевая безопасность:
- Межсетевые экраны (Firewall).
- VPN для удалённого доступа.
- Мониторинг сетевых атак (SIEM-системы).

Практическая часть
Задание 1. Анализ требований по уровням защиты
Изучите ГОСТ Р 56939-2024 (можно найти на сайте Росстандарта).
Заполните таблицу, сравнив требования для разных уровней ИСПДн:

Требование	1-й уровень (высокий)	2-й уровень (средний)	3-й уровень (низкий)
Шифрование данных	Обязательно (ГОСТ 28147-89)	Рекомендуется	Не требуется

Требование	1-й уровень (высокий)	2-й уровень (средний)	3-й уровень (низкий)
Аутентификация пользователей	Двухфакторная	Парольная	Упрощённая
Резервное копирование	Ежедневно + автономное	Еженедельно	По необходимости

Задание 2. Разбор кейса
Ситуация: Компания "Данные+" обрабатывает ПДн клиентов (ФИО, паспортные данные, номера телефонов). Система относится ко 2-му уровню угроз.
Вопросы:

- Какие меры защиты обязательны согласно ГОСТ Р 56939-2024?
- Какие документы нужно разработать? (Политика безопасности, регламенты доступа и т. д.)
- Какие технические средства необходимо внедрить?

Задание 3. Практическое применение
Задача: Вы – специалист по ИБ. В организации внедряется новая CRM-система для хранения ПДн сотрудников (2-й уровень).
Требуется:

- Составить чек-лист мер защиты по ГОСТ Р 56939-2024.
- Предложить 3 технических решения (например, СКЗИ, DLP-система).
- Оценить риски при несоблюдении стандарта (штрафы по ст**. 13.11 КоАП РФ**).

Нормативно-правовые акты РФ

1. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Основной закон, регулирующий вопросы ИБ в РФ)
2. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"(Регламентирует обработку и защиту ПДн)
3. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)" (Требования к защите объектов КИИ)
4. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности РФ" (Стратегические направления защиты информации в России)

ГОСТы и стандарты

1. ГОСТ Р ИСО/МЭК 27001-2022 "Информационная безопасность. Системы менеджмента информационной безопасности. Требования" (Международный стандарт, адаптированный для РФ)
2. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций" (Требования к защите информации в банковской сфере)

3. Приказ ФСТЭК России № 17 от 11.02.2013 "Требования по защите информации в государственных информационных системах"

Учебные пособия и монографии

1. Галатенко В.А. "Основы информационной безопасности" (Учебник для вузов, охватывающий правовые и организационные аспекты ИБ)
2. Петренко С.А., Курбатов В.А. "Политика информационной безопасности компании" (Практическое руководство по разработке и внедрению политик ИБ)
3. Шаньгин В.Ф. "Информационная безопасность компьютерных систем и сетей" (Рассматривает правовые основы защиты информации в IT-инфраструктуре)

Дополнительные источники

1. NIST SP 800-53 (США) – Стандарт по управлению рисками ИБ
2. ISO/IEC 27005:2022 – Международный стандарт по оценке рисков
3. Материалы ФСБ России и ФСТЭК (методические рекомендации)

Примечание:
Для подготовки работ рекомендуется использовать официальные сайты:
ФСТЭК России
Росстандарт
КонсультантПлюс (для проверки актуальности законов)