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

Методические указания

по выполнению лабораторных работ
по дисциплине
«ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОБЪЕКТАХ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ»
для студентов специальности 10.05.03 Информационная безопасность автоматизированных систем,
специализация «Анализ безопасности информационных систем»

Ставрополь
2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Цель и задачи освоения дисциплины

Целью освоения дисциплины «Обеспечение информационной безопасности на объектах критической информационной инфраструктуры» является формирование у будущего специалиста по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация «Анализ безопасности информационных систем» системных знаний и практических навыков по защите информации и информационных систем, составляющих критическую информационную инфраструктуру. Дисциплина направлена на освоение нормативно-правовой базы, методов и средств обеспечения конфиденциальности, целостности и доступности информации, а также на развитие умений выявлять угрозы, оценивать риски и внедрять комплексные меры защиты для обеспечения устойчивого и безопасного функционирования объектов КИИ в условиях современных киберугроз.

СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Лабораторная работа 1. Обеспечение информационной безопасности на объектах критической информационной инфраструктуры.

Цель работы
Научиться собирать и систематизировать сведения о структуре организации, выявлять потенциальные объекты критической информационной инфраструктуры (КИИ) и определять их роль в критических процессах организации.

Задачи
- Изучить структуру организации и ее информационные ресурсы.
- Определить объекты, которые могут быть отнесены к КИИ.
- Оценить роль выявленных объектов в обеспечении критических процессов организации.
- Сформировать первичные сведения для последующего категорирования и анализа угроз.

Теоретическая основа
Критическая информационная инфраструктура (КИИ) — это совокупность информационных систем, сетей и ресурсов, обеспечивающих жизненно важные функции и процессы организации, нарушение которых может привести к серьезным последствиям для безопасности, экономики и общества.
Сбор сведений об организации включает анализ организационной структуры, информационных систем, автоматизированных систем управления и сетей, а также выявление объектов, обеспечивающих критические процессы.

Оборудование и материалы
- Документы организации (структурные схемы, регламенты, ИТ-инвентаризация)
- Средства для сбора информации (опросники, интервью с сотрудниками)
- Методические материалы по КИИ и безопасности значимых объектов

Ход работы

1. Сбор информации о структуре организации

- Получить организационную схему и описание основных подразделений.
- Определить ключевые бизнес-процессы и их информационное обеспечение.
- Выявить используемые информационные системы, автоматизированные системы управления, сети и коммуникационные средства.

2. Идентификация потенциальных объектов КИИ

- На основе собранных данных выделить объекты, критически важные для функционирования организации (например, серверы, базы данных, системы управления технологическими процессами).
- Определить значимость каждого объекта для обеспечения непрерывности критических процессов.

3. Определение роли объектов в критических процессах

- Оценить, какие процессы зависят от каждого объекта.
- Определить последствия нарушения функционирования объектов для организации.
- Сформировать перечень объектов с указанием их роли и значимости.

4. Подготовка отчета

- Систематизировать результаты в виде отчета с описанием структуры организации, выявленных объектов КИИ и их роли.
- Рекомендовать дальнейшие шаги по категорированию и обеспечению безопасности объектов.

Вопросы для самоконтроля

- Что относится к критической информационной инфраструктуре организации?
- Какие методы используются для сбора сведений об организации?
- Как определить значимость объекта КИИ?
- Какие последствия могут возникнуть при нарушении функционирования объектов КИИ?

Список основной литературы

- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
- Корниенко А. А., Глухов А. П., Корниенко С. В. *Категорирование и обеспечение безопасности значимых объектов критической информационной инфраструктуры*.
- *Управление безопасностью критических информационных инфраструктур*, 2021, ISBN 978-5-9912-0916-8.

Список дополнительной литературы

- Методические рекомендации по обеспечению безопасности значимых объектов КИИ (ФСТЭК России).
- Мосполитех, учебно-методические материалы по безопасности критической информационной инфраструктуры.
- Рекомендации по защите критической информационной инфраструктуры, Security Vision

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org
6. http://keirsey.com

Лабораторная работа 2. Создание комиссии по категорированию объектов КИИ.

Цель работы

Освоить процесс формирования комиссии по категорированию объектов критической информационной инфраструктуры (КИИ), включая разработку состава комиссии, распределение ролей и подготовку приказа о создании комиссии.

Задачи

- Изучить нормативные требования к созданию комиссии по категорированию объектов КИИ.
- Разработать состав комиссии с учетом функциональных обязанностей и компетенций участников.
- Сформировать проект приказа о создании комиссии с указанием целей, задач и полномочий.
- Ознакомиться с регламентом работы комиссии и подготовить рекомендации по ее деятельности.

Теоретическая основа

Категорирование объектов КИИ — обязательная процедура для субъектов критической информационной инфраструктуры, направленная на определение уровня значимости объектов и обеспечение их безопасности. Для организации процесса категорирования создается комиссия, которая действует на постоянной основе и включает специалистов из различных подразделений организации.

Состав комиссии формируется руководителем организации или уполномоченным им лицом и должен включать представителей ключевых направлений: информационных технологий, безопасности, эксплуатации технологического оборудования и др.

Приказ о создании комиссии является локальным нормативным актом, регламентирующим ее создание, состав, полномочия и задачи.

Оборудование и материалы

- Нормативные документы по КИИ (Федеральный закон № 187-ФЗ, методические рекомендации ФСТЭК).
- Шаблоны приказов и положений о комиссии.
- Примеры организационных структур и должностных инструкций.

Ход работы

1. Изучение нормативной базы

- Ознакомиться с Федеральным законом № 187-ФЗ и методическими рекомендациями по категорированию объектов КИИ.
- Выделить требования к составу комиссии и процедуре ее создания.

2. Разработка состава комиссии

- Определить руководителя комиссии (руководитель организации или уполномоченное им лицо, например, заместитель по безопасности).
- Включить в состав специалистов:
    - Экспертов в области информационных технологий и связи (администраторов, ИТ-специалистов).
    - Специалистов по эксплуатации технологического оборудования и промышленной безопасности.
    - Сотрудников, отвечающих за информационную безопасность.
    - При необходимости — представителей подразделений по защите государственной тайны, гражданской обороне, финансово-экономического и юридического отделов.

3. Распределение ролей в комиссии

- Председатель комиссии — руководитель организации или уполномоченное лицо.
- Заместитель председателя — сотрудник, курирующий вопросы безопасности.
- Члены комиссии — специалисты по направлениям деятельности, участвующие в категорировании.

4. Подготовка приказа о создании комиссии

- Оформить приказ с указанием:
    - Наименования комиссии и цели ее создания.
    - Состав комиссии с указанием должностей и ФИО.
    - Полномочий и задач комиссии (определение критических процессов, выявление объектов КИИ, анализ угроз и пр.).
    - Сроков выполнения основных этапов работы.
    - Утверждение положения и плана работы комиссии.

5. Ознакомление с положением о комиссии и планом работы

- Рекомендовать разработать положение, регламентирующее деятельность комиссии.
- Сформировать план работы на ближайший период (определение процессов, выявление объектов, анализ угроз, подготовка отчетов).

6. Итог

- Представить проект приказа и состав комиссии преподавателю для проверки.
- Обсудить возможные сложности при формировании комиссии и распределении ролей.

Пример структуры приказа о создании комиссии

Приказ № ___
«__» _____ 20__ г.

О создании комиссии по категорированию объектов критической информационной инфраструктуры

В целях выполнения требований Федерального закона № 187-ФЗ и методических рекомендаций по категорированию объектов КИИ:

1. Создать комиссию по категорированию объектов КИИ в составе:

- Председатель комиссии: (должность, ФИО)
- Заместитель председателя: (должность, ФИО)
- Члены комиссии:
  (должность, ФИО)
  (должность, ФИО)
  ...

2. Утвердить Положение о комиссии и План работы комиссии.

3. Комиссии в срок до «__» _____ 20__ г.:
- Определить критические процессы деятельности организации;
- Выявить объекты КИИ, подлежащие категорированию;
- Проанализировать угрозы безопасности информации;
- Подготовить предложения для утверждения перечня объектов КИИ.

4. Контроль за исполнением настоящего приказа возложить на (должность).

Руководитель организации: _____ (подпись, ФИО)

Вопросы для самоконтроля

- Кто может возглавлять комиссию по категорированию объектов КИИ?
- Какие специалисты должны входить в состав комиссии?
- Какие основные задачи возлагаются на комиссию?
- Какие документы оформляются при создании и работе комиссии?

Список основной литературы

- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Методические рекомендации по категорированию объектов КИИ, ФСТЭК России (2024).
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов КИИ».
- Руководство по обеспечению информационной безопасности на объектах КИИ, 2023.

Список дополнительной литературы

- Методические рекомендации по созданию и работе комиссий по категорированию объектов КИИ, Минтранс России, 2023.
- Учебное пособие «Обеспечение безопасности критической информационной инфраструктуры», Мосполитех, 2022.
- Практическое руководство по информационной безопасности и категорированию объектов, 2021.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование

Лабораторная работа 3. Формирование перечня объектов КИИ и их категорирование

Цель работы

Научиться выделять и описывать объекты критической информационной инфраструктуры (КИИ), проводить их категорирование по установленным критериям значимости и оформлять необходимые документы по итогам работы.

Задачи

- Изучить понятие и виды объектов КИИ.
- Провести инвентаризацию и выделение объектов КИИ в рамках заданной организации или автоматизированной системы.
- Оценить значимость объектов по критериям, установленным законодательством и методическими рекомендациями.
- Сформировать перечень объектов КИИ с присвоением категорий значимости.
- Оформить протокол категорирования и другие необходимые документы.

Теоретическая основа

Объекты КИИ — это информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, которые обеспечивают выполнение критически важных процессов в организации. В соответствии с Федеральным законом № 187-ФЗ и постановлением Правительства РФ № 127 объекты КИИ подлежат категорированию, то есть присвоению одной из трех категорий значимости (первая — максимальная, вторая, третья — минимальная) на основе оценки потенциального ущерба для жизни, экономики, экологии, безопасности и политики.

Категорирование проводится комиссией, которая анализирует критические процессы, выявляет объекты КИИ, оценивает угрозы и последствия нарушения их функционирования.

Оборудование и материалы

- Организационные документы и схемы автоматизированных систем.
- Нормативные документы: Федеральный закон № 187-ФЗ, постановление Правительства РФ № 127, методические рекомендации ФСТЭК.
- Формы и шаблоны протоколов категорирования.

Ход работы

1. Изучение объекта исследования

- Выбрать организацию или автоматизированную информационную систему (АИС) для анализа.
- Описать назначение АИС, ключевые процессы, которые она автоматизирует, и состав оборудования (серверы, сети, рабочие станции и т.п.).

2. Выделение объектов КИИ

- Провести инвентаризацию информационных систем, сетей и автоматизированных систем управления, используемых в организации.
- Определить объекты, обеспечивающие критические процессы (управленческие, технологические, производственные, финансово-экономические и др.).
- Сформировать предварительный перечень объектов КИИ.

3. Проведение категорирования объектов КИИ

- Создать комиссию по категорированию (если она еще не создана).
- Определить критерии значимости объектов по пяти основным сферам: социум, экономика, экология, безопасность, политика.
- Оценить потенциальный ущерб и последствия нарушения функционирования каждого объекта.
- Присвоить объектам одну из трех категорий значимости:
    - Первая категория — объекты с максимальным уровнем значимости (например, нарушение работы повлияет на миллионы пользователей или критически важные процессы).
    - Вторая категория — объекты со средним уровнем значимости.
    - Третья категория — объекты с минимальным уровнем значимости, но подлежащие защите.

4. Оформление документов

- Составить протокол категорирования с описанием объекта, критериев оценки, присвоенной категории и обоснования.
- Подготовить акт формирования перечня объектов КИИ.
- Сформировать отчет с результатами категорирования и рекомендациями по обеспечению безопасности.

5. Представление результатов

- Представить сформированный перечень объектов КИИ с категориями значимости.
- Обсудить возможные угрозы и меры защиты для объектов с разными категориями.

Вопросы для самоконтроля

- Какие виды объектов относятся к КИИ?
- Какие критерии используются для присвоения категории значимости объекту КИИ?
- Каковы основные этапы процесса категорирования?
- Какие документы оформляются по итогам категорирования?

Пример структуры протокола категорирования

Параметр	Описание
Наименование объекта КИИ	Например, «Автоматизированная система управления цехом»
Описание объекта	Назначение, состав, используемое оборудование
Критические процессы	Перечень процессов, обеспечиваемых объектом
Критерии значимости	Социум, экономика, экология, безопасность, политика
Оценка потенциального ущерба	Краткое описание возможных последствий
Присвоенная категория	Первая, вторая или третья
Обоснование категории	Аргументация выбора категории

Дата и подписи комиссии	Дата проведения и подписи членов комиссии

Список основной литературы

- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры».
- Методические рекомендации по категорированию объектов КИИ, ФСТЭК России, 2023.
- Безопасность объектов критической информационной инфраструктуры: учебное пособие / Под ред. А.А. Корниенко. — М., 2022.

Список дополнительной литературы

- Руководство по обеспечению информационной безопасности на объектах КИИ, Мосполитех, 2021.
- Практическое руководство по категорированию объектов КИИ, 2023.
- Методические материалы ФСТЭК России по моделированию угроз и оценке рисков безопасности информации.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование

Лабораторная работа 4. Анализ возможных действий нарушителей в отношении объектов КИИ

Цель работы

Освоить методы построения моделей нарушителей, провести анализ их потенциальных действий и сценариев атак на объекты критической информационной инфраструктуры (КИИ) с целью выявления угроз и оценки рисков.

Задачи

- Изучить классификацию и характеристики нарушителей, актуальные для объектов КИИ.
- Построить модели нарушителей с учетом их возможностей, мотиваций и ресурсов.
- Проанализировать возможные действия нарушителей и типовые сценарии атак на объекты КИИ.
- Оценить потенциальные последствия реализации угроз безопасности информации.

- Подготовить отчет с результатами анализа и рекомендациями по минимизации рисков.

Теоретическая основа
Обеспечение безопасности объектов КИИ требует системного подхода к анализу угроз, исходящих от различных категорий нарушителей. Нарушители классифицируются по уровню профессиональной подготовки, технических возможностей, мотивации и правам доступа (внутренние и внешние). Модели нарушителей и угроз позволяют систематизировать информацию о потенциальных атаках и разрабатывать эффективные меры защиты.

Оборудование и материалы
- Нормативные документы по безопасности КИИ (Федеральный закон №187-ФЗ, Приказ ФСТЭК №239).
- Методические материалы по моделированию угроз и нарушителей.
- Примеры типовых сценариев атак и моделей нарушителей.
- Средства для оформления отчетной документации.

Ход работы
1. Изучение характеристик нарушителей
- Рассмотреть классификацию нарушителей по уровню возможностей: базовый, повышенный, средний, высокий.
- Определить категории нарушителей: внутренние (с правами доступа) и внешние (без прав доступа).
- Проанализировать мотивации и ресурсы каждой категории.

2. Построение моделей нарушителей
- Сформировать описание моделей нарушителей для выбранного объекта КИИ, учитывая:
    - Цели и мотивацию нарушителя.
    - Технические и организационные возможности.
    - Каналы и методы доступа к объекту.

3. Анализ возможных действий и сценариев атак
- Определить потенциальные действия нарушителей (несанкционированный доступ, модификация данных, отказ в обслуживании и др.).
- Составить типовые сценарии атак, учитывая последовательность действий и используемые методы.
- Оценить уязвимости объекта КИИ, которые могут быть использованы нарушителями.

4. Оценка последствий реализации угроз
- Проанализировать возможные последствия для безопасности, экономики, общества и государства при успешной атаке.
- Оценить масштаб и серьезность ущерба.

5. Подготовка отчета
- Систематизировать результаты анализа в отчете, включающем:
    - Описание моделей нарушителей.
    - Перечень возможных действий и сценариев атак.
    - Оценку рисков и последствий.
    - Рекомендации по снижению угроз.

Вопросы для самоконтроля

- Какие категории нарушителей существуют в контексте КИИ?
- Каковы основные характеристики моделей нарушителей?
- Какие типовые сценарии атак наиболее распространены на объекты КИИ?
- Как оценить последствия реализации угроз безопасности информации?
- Какие меры можно рекомендовать для минимизации рисков?

Список основной литературы

- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
- Учебник «Безопасность критической информационной инфраструктуры», Мосполитех, 2022.
- Методические рекомендации ФСТЭК России по моделированию угроз и нарушителей, 2021.

Список дополнительной литературы

- Руководство по обеспечению безопасности объектов КИИ, 2023.
- Практическое пособие по анализу угроз и управлению рисками в информационной безопасности, 2021.
- Учебное пособие «Обеспечение безопасности критических информационных инфраструктур», 2024.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование

Лабораторная работа 5. Разработка модели угроз для объектов КИИ

Цель работы

Научиться разрабатывать модель угроз для конкретного объекта критической информационной инфраструктуры (КИИ), включающую идентификацию актуальных угроз, оценку их вероятности и построение дерева угроз.

Задачи

- Изучить методики моделирования угроз безопасности информации, применяемые к объектам КИИ.

- Идентифицировать потенциальные угрозы безопасности информации для выбранного объекта КИИ.
- Оценить актуальность выявленных угроз с учетом характеристик объекта и возможных нарушителей.
- Построить дерево угроз, отражающее возможные пути реализации угроз и их взаимосвязи.
- Подготовить отчет с описанием модели угроз и рекомендациями по ее использованию для разработки мер защиты.

Теоретическая основа

Модель угроз безопасности информации – это систематизированное описание потенциальных угроз, актуальных для конкретного объекта КИИ, с учетом характеристик объекта, возможных нарушителей и уязвимостей. Моделирование угроз позволяет определить наиболее вероятные сценарии атак и разработать эффективные меры защиты, соответствующие специфике объекта. Дерево угроз – это графическое представление возможных путей реализации угроз, которое помогает визуализировать взаимосвязи между различными угрозами и уязвимостями.

Оборудование и материалы

- Нормативные документы по безопасности КИИ (Федеральный закон № 187-ФЗ, Приказ ФСТЭК № 239).
- Методические рекомендации по моделированию угроз безопасности информации.
- Программное обеспечение для построения деревьев угроз (например, Microsoft Visio, yEd Graph Editor).
- Шаблоны для оформления отчетов.

Ход работы

1. **Выбор объекта КИИ**
    - Определите конкретный объект КИИ, для которого будет разрабатываться модель угроз (например, автоматизированная система управления технологическим процессом на электростанции).
    - Опишите назначение и структуру объекта, выделите ключевые компоненты и процессы.
2. **Идентификация угроз**
    - Изучите перечень угроз безопасности информации, актуальных для объектов КИИ, используя нормативные документы, методические рекомендации и базы данных угроз (например, Банк данных угроз ФСТЭК России).
    - Определите угрозы, которые могут быть реализованы в отношении выбранного объекта, с учетом его специфики и возможных уязвимостей.
3. **Оценка актуальности угроз**
    - Оцените вероятность реализации каждой угрозы, учитывая:
        - Возможности и мотивацию потенциальных нарушителей.
        - Наличие уязвимостей в объекте КИИ.
        - Эффективность существующих мер защиты.
    - Присвойте каждой угрозе уровень актуальности (например, высокий, средний, низкий).
4. **Построение дерева угроз**
    - Для наиболее актуальных угроз постройте дерево угроз, отражающее возможные пути их реализации.

- Начните с корневой угрозы и разбейте ее на под угрозы, представляющие собой отдельные шаги или условия, необходимые для реализации основной угрозы.
- Продолжайте декомпозицию до тех пор, пока не будут выявлены конкретные уязвимости или действия, которые могут привести к реализации угрозы.

5. **Оформление отчета**
   - Опишите выбранный объект КИИ и его ключевые характеристики.
   - Приведите перечень идентифицированных угроз и оценку их актуальности.
   - Представьте деревья угроз для наиболее актуальных угроз.
   - Сформулируйте рекомендации по использованию разработанной модели угроз для разработки мер защиты информации, включая технические, организационные и правовые меры.

Пример структуры отчета

1. Введение
   - Описание объекта КИИ
   - Цель и задачи моделирования угроз
2. Идентификация угроз
   - Перечень идентифицированных угроз
   - Оценка актуальности угроз
3. Деревья угроз
   - Дерево угроз для угрозы 1
   - Дерево угроз для угрозы 2
   - И т.д.
4. Рекомендации
   - Технические меры защиты
   - Организационные меры защиты
   - Правовые меры защиты
5. Заключение

Вопросы для самоконтроля

- Какие основные этапы включает процесс моделирования угроз безопасности информации?
- Какие факторы необходимо учитывать при оценке актуальности угроз?
- Как построить дерево угроз и какую информацию оно должно содержать?
- Какие типы мер защиты информации могут быть рекомендованы на основе модели угроз?
- В соответствии с каким документом для значимых объектов КИИ должна проводиться оценка угроз ИБ?

Список основной литературы

- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
- Методика оценки угроз безопасности информации, утвержденная ФСТЭК России 05.02.2021.
- Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. *Управление безопасностью критических информационных инфраструктур*.

Список дополнительной литературы

- Официальный сайт ФСТЭК России (разделы, посвященные безопасности КИИ).
- База данных угроз безопасности информации ФСТЭК России.
- Курс «Критическая информационная инфраструктура».
- Учебное пособие «Безопасность критической информационной инфраструктуры», 2022.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. https://urait.ru/bcode/449575 – Зенкина, С. В. Сетевая проектно-исследовательская деятельность обучающихся : учебное пособие для вузов / С. В. Зенкина, Е. К. Герасимова, О. П. Панкратова. — Москва : Издательство Юрайт, 2020. — 152 с. — (Высшее образование). — ISBN 978-5-534-13229-8. — Текст : электронный // ЭБС Юрайт [сайт].

Лабораторная работа 6. Оценка уязвимостей объектов КИИ

Цель работы

Освоить методы выявления, анализа и оценки уязвимостей программных, аппаратных и организационных компонентов объектов критической информационной инфраструктуры (КИИ) с использованием современных методик и инструментов.

Задачи

- Изучить классификацию уязвимостей в программных, аппаратных и организационных компонентах КИИ.
- Провести сбор информации и идентификацию уязвимостей выбранного объекта КИИ.
- Оценить уровень критичности выявленных уязвимостей с применением методики CVSS (Common Vulnerability Scoring System).
- Проанализировать влияние уязвимостей на конфиденциальность, целостность и доступность информации.
- Подготовить отчет с результатами оценки уязвимостей и рекомендациями по их устранению.

Теоретическая основа

Уязвимости — это слабые места в программных, аппаратных и организационных компонентах, которые могут быть использованы злоумышленниками для реализации угроз безопасности. Оценка уязвимостей проводится с использованием стандартизированных методик, таких как CVSS, которая учитывает базовые, временные и контекстные метрики для определения уровня риска. Анализ уязвимостей позволяет приоритизировать меры защиты и минимизировать потенциальные риски для объектов КИИ.

Оборудование и материалы

- Документация и описание объекта КИИ (структура, используемые системы и оборудование).
- Средства автоматизированного анализа уязвимостей (например, OpenVAS, Nessus, Solar appScreener).
- Методические документы ФСТЭК России по оценке уязвимостей.
- Онлайн-калькулятор CVSS v3 для оценки критичности уязвимостей.

Ход работы

1. Подготовительный этап

- Ознакомиться с объектом КИИ, его программными, аппаратными и организационными компонентами.
- Изучить нормативные документы и методики оценки уязвимостей (например, CVSS).

2. Сбор информации и идентификация уязвимостей

- Провести сбор информации о программном обеспечении, оборудовании и организационных процессах объекта.
- Использовать автоматизированные инструменты для сканирования и выявления уязвимостей в программных и аппаратных компонентах.
- Проанализировать организационные процессы на предмет возможных уязвимостей (например, недостатки в политике безопасности, недостаточная квалификация персонала).

3. Оценка уровня критичности уязвимостей

- Для каждой выявленной уязвимости определить базовые метрики CVSS: вектор атаки, сложность атаки, уровень привилегий, влияние на конфиденциальность, целостность и доступность.
- Рассчитать итоговый балл критичности уязвимости по шкале CVSS (от 0 до 10).
- Классифицировать уязвимости по уровням критичности: низкий (0,1–3,9), средний (4–6,9), высокий (7–8,9), критический (9–10).

4. Анализ влияния уязвимостей на безопасность объекта

- Оценить потенциальные последствия эксплуатации уязвимостей для конфиденциальности, целостности и доступности информации.
- Определить приоритеты устранения уязвимостей с учетом их критичности и влияния на объект.

5. Подготовка отчета

- Систематизировать результаты в отчете, включающем:
    - Описание объекта КИИ и исследуемых компонентов.
    - Перечень выявленных уязвимостей с их характеристиками.
    - Результаты оценки критичности по CVSS.
    - Анализ влияния уязвимостей на безопасность.
    - Рекомендации по устранению и минимизации рисков.

Вопросы для самоконтроля

- Какие категории уязвимостей существуют в программных, аппаратных и организационных компонентах?
- Каковы основные метрики CVSS и как они влияют на оценку критичности уязвимости?
- Какие инструменты используются для автоматизированного выявления уязвимостей?

- Как оценить влияние уязвимости на конфиденциальность, целостность и доступность информации?
- Какие меры можно рекомендовать для снижения рисков, связанных с выявленными уязвимостями?

Список основной литературы

- Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств, ФСТЭК России, 28 октября 2022 г.
- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов КИИ».
- Common Vulnerability Scoring System v3.1 (CVSS), FIRST.org, 2019.

Список дополнительной литературы

- Руководство по оценке уязвимостей и управлению рисками, Security Vision, 2023.
- Практическое руководство по информационной безопасности, Мосполитех, 2021.
- Методика оценки угроз безопасности информации, ФСТЭК России.
- Solar appScreener: инструменты для анализа уязвимостей программного обеспечения.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование

Лабораторная работа 7. Оценка рисков для объектов КИИ

Цель работы

Освоить методы комплексной оценки рисков безопасности для объектов критической информационной инфраструктуры (КИИ) на основе анализа выявленных угроз и уязвимостей, а также определить приоритетные направления защиты для минимизации рисков.

Задачи

- Изучить основные понятия и методики оценки рисков в области информационной безопасности КИИ.
- Провести систематизацию выявленных угроз и уязвимостей выбранного объекта КИИ.

- Рассчитать уровень рисков с использованием качественных и количественных методов, включая метрики CVSS и оценку потенциала нарушителя.
- Определить приоритетные направления и меры защиты на основе результатов оценки рисков.
- Подготовить отчет с результатами оценки и рекомендациями по управлению рисками.

Теоретическая основа

Оценка рисков информационной безопасности представляет собой процесс определения вероятности реализации угроз и последствий их воздействия на объекты КИИ с учетом существующих уязвимостей и характеристик нарушителей. Современные методики включают комбинированный (гибридный) подход, сочетающий количественные и качественные методы оценки. Важным элементом оценки является использование стандарта CVSS для оценки уязвимостей и ГОСТ Р ИСО/МЭК 18045-2013 для оценки потенциала нарушителя. Результаты оценки рисков служат основой для выбора и адаптации мер защиты, направленных на снижение вероятности и последствий инцидентов.

Оборудование и материалы

- Описание и характеристики выбранного объекта КИИ.
- Перечень выявленных угроз и уязвимостей объекта.
- Методические рекомендации ФСТЭК России по оценке рисков.
- Инструменты для расчета CVSS (например, онлайн-калькуляторы).
- Таблицы и шаблоны для систематизации данных и оформления отчета.

Ход работы

1. Подготовка исходных данных

- Ознакомиться с характеристиками объекта КИИ, включая его структуру, функции и критические процессы.
- Систематизировать выявленные угрозы и уязвимости, связанные с объектом.

2. Оценка уязвимостей по CVSS

- Для каждой уязвимости определить базовые метрики CVSS: вектор атаки, сложность атаки, уровень привилегий, влияние на конфиденциальность, целостность и доступность.
- Рассчитать итоговый балл критичности уязвимости.

3. Оценка потенциала нарушителя

- Оценить характеристики потенциального нарушителя согласно ГОСТ Р ИСО/МЭК 18045-2013: уровень знаний, ресурсов, возможностей доступа и мотивации.

4. Расчет уровня риска

- Определить вероятность реализации каждой угрозы с учетом уязвимостей и потенциала нарушителя.
- Оценить тяжесть последствий для безопасности объекта (конфиденциальность, целостность, доступность).
- Рассчитать уровень риска как функцию вероятности и тяжести последствий.

5. Приоритизация рисков и определение направлений защиты

- Сгруппировать риски по уровням критичности (низкий, средний, высокий, критический).
- Определить приоритетные риски, требующие немедленного внимания.
- Разработать рекомендации по выбору технических, организационных и административных мер защиты для снижения приоритетных рисков.

6. Оформление итогового отчета

- Представить систематизированные данные по угрозам, уязвимостям и оценке рисков.
- Включить таблицы с результатами расчетов CVSS и оценки потенциала нарушителя.
- Описать приоритетные направления защиты и меры по управлению рисками.

Вопросы для самоконтроля

- Какие методы оценки рисков применяются для объектов КИИ?
- Как использовать метрики CVSS при оценке уязвимостей?
- Какие характеристики учитываются при оценке потенциала нарушителя?
- Как рассчитывается уровень риска и на что он влияет?
- Какие критерии используются для приоритизации рисков?
- Какие меры защиты наиболее эффективны для снижения приоритетных рисков?

Список основной литературы

- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры».
- Иваненко В. Г., Иванова Н. Д. «Оценка рисков информационной безопасности автоматизированных систем управления технологическим процессом», 2024.
- Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств, ФСТЭК России, 2022.
- Common Vulnerability Scoring System v3.1 (CVSS), FIRST.org, 2019.
- ГОСТ Р ИСО/МЭК 18045-2013 «Информационная технология. Методы оценки безопасности. Оценка потенциала нападения нарушителя».

Список дополнительной литературы

- Руководство по управлению рисками информационной безопасности, Security Vision, 2023.
- Практическое руководство по обеспечению безопасности объектов КИИ, Мосполитех, 2021.
- Методические рекомендации ФСТЭК России по оценке угроз и уязвимостей.
- Учебное пособие «Обеспечение безопасности критической информационной инфраструктуры», 2022.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование

Лабораторная работа 8. Выбор и обоснование средств защиты информации

Цель работы

Научиться анализировать актуальные угрозы безопасности информации для объектов критической информационной инфраструктуры (КИИ), подбирать технические и программные средства защиты, а также обосновывать их применение с целью нейтрализации выявленных угроз и обеспечения устойчивого функционирования объектов.

Задачи

- Изучить классификацию и характеристики технических и программных средств защиты информации, применяемых на объектах КИИ.
- Проанализировать актуальные угрозы и уязвимости выбранного объекта КИИ.
- Подобрать соответствующие средства защиты, учитывая специфику объекта и виды угроз.
- Обосновать выбор средств защиты с точки зрения их эффективности, совместимости и соответствия нормативным требованиям.
- Подготовить отчет с описанием выбранных средств защиты и рекомендациями по их внедрению.

Теоретическая основа

Обеспечение безопасности объектов КИИ — комплексный процесс, включающий технические, программные и организационные меры, направленные на предотвращение компьютерных атак, несанкционированного доступа, модификации, уничтожения и утечки информации. Средства защиты информации включают системы идентификации и аутентификации, управление доступом, антивирусные комплексы, системы обнаружения и предотвращения вторжений, шифрование, аудит безопасности, защиту машинных носителей и др. Выбор средств защиты должен базироваться на анализе угроз, уязвимостей и категории значимости объекта, а также соответствовать требованиям законодательства и нормативных актов (Федеральный закон № 187-ФЗ, Приказы ФСТЭК).

Оборудование и материалы

- Описание выбранного объекта КИИ (структура, используемые системы, процессы).
- Перечень выявленных угроз и уязвимостей объекта.
- Нормативные документы по безопасности КИИ (Федеральный закон № 187-ФЗ, Приказ ФСТЭК № 239 и др.).
- Каталоги и описания технических и программных средств защиты информации.
- Шаблоны для оформления отчета.

Ход работы

1. Анализ объекта и выявленных угроз

- Изучите структуру и функциональные особенности объекта КИИ.
- Систематизируйте актуальные угрозы и уязвимости, выявленные на предыдущих этапах анализа безопасности.

2. Обзор средств защиты информации

- Ознакомьтесь с основными видами технических и программных средств защиты, применяемых на объектах КИИ:
    - Идентификация и аутентификация пользователей (ИАФ).
    - Управление доступом (УПД).
    - Антивирусная защита (АВЗ).
    - Системы предотвращения вторжений (СОВ).

    - Шифрование и обеспечение целостности данных (ОЦЛ).
    - Аудит безопасности (АУД).
    - Защита машинных носителей информации (ЗНИ).
- Рассмотрите особенности применения каждого средства в контексте выбранного объекта.

3. Подбор средств защиты

- На основе анализа угроз и уязвимостей определите, какие средства защиты наиболее эффективны для нейтрализации конкретных угроз.
- Учитывайте требования к совместимости, масштабируемости и соответствию нормативным актам.
- Обоснуйте выбор каждого средства с точки зрения его функциональных возможностей и ожидаемой эффективности.

4. Формирование рекомендаций по внедрению

- Опишите этапы внедрения выбранных средств защиты на объекте КИИ.
- Укажите требования к техническому обеспечению и квалификации персонала.
- Предложите меры по контролю и мониторингу эффективности защиты.

5. Оформление отчета

- Включите в отчет:
    - Краткое описание объекта и выявленных угроз.
    - Перечень выбранных средств защиты с обоснованием.
    - Рекомендации по внедрению и эксплуатации.
    - Заключение о соответствии выбранных средств требованиям безопасности.

Вопросы для самоконтроля

- Какие основные виды технических и программных средств защиты информации применяются на объектах КИИ?
- Как соотнести выбор средств защиты с анализом угроз и уязвимостей?
- Какие нормативные требования необходимо учитывать при подборе средств защиты?
- Какие факторы влияют на эффективность выбранных средств защиты?
- Как организовать внедрение и контроль работы средств защиты?

Список основной литературы

- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры».
- Методические рекомендации ФСТЭК России по выбору и применению средств защиты информации на объектах КИИ, 2023.
- Учебное пособие «Обеспечение безопасности критической информационной инфраструктуры», Мосполитех, 2022.

Список дополнительной литературы

- Руководство по защите информации на объектах КИИ, Security Vision, 2023.
- Практическое руководство по информационной безопасности, Мосполитех, 2021.
- Методика оценки и выбора средств защиты информации, ФСТЭК России, 2022.
- Каталоги и технические описания современных средств защиты информации (российские и международные производители).

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование

Лабораторная работа 9. Разработка организационно-распорядительных документов по ИБ на объектах КИИ

Цель работы

Освоить процесс составления ключевых организационно-распорядительных документов (регламентов, инструкций, положений), необходимых для обеспечения информационной безопасности на объектах критической информационной инфраструктуры (КИИ), с учетом требований законодательства и нормативных актов.

Задачи

- Изучить структуру и назначение основных организационно-распорядительных документов по ИБ на объектах КИИ.
- Ознакомиться с требованиями Федерального закона № 187-ФЗ и приказов ФСТЭК России, регламентирующих документооборот в области безопасности КИИ.
- Разработать проект основных документов:
    - Регламент по обеспечению информационной безопасности;
    - Инструкцию по действиям персонала при обеспечении безопасности;
    - Положение о системе безопасности объекта КИИ.
- Обосновать содержание и структуру разработанных документов.
- Подготовить отчет с результатами работы и рекомендациями по внедрению документов.

Теоретическая основа

Организационно-распорядительные документы являются фундаментом системы управления информационной безопасностью на объектах КИИ. Они формализуют политику безопасности, распределяют обязанности и ответственность, определяют процедуры и правила действий персонала, а также регламентируют взаимодействие подразделений и контроль исполнения мер защиты. Требования к таким документам установлены в Федеральном законе № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», а также в приказах ФСТЭК России (например, № 235 и № 239 от 2017 года).

Документация должна охватывать:

- цели и задачи обеспечения безопасности;
- описание объекта и его критических компонентов;
- организационную структуру и распределение ответственности;

- процедуры выявления и реагирования на инциденты;
- требования к техническим и организационным мерам защиты.

Оборудование и материалы

- Нормативные документы: Федеральный закон № 187-ФЗ, приказы ФСТЭК № 235 и № 239.
- Примеры и шаблоны организационно-распорядительных документов (регламенты, инструкции, положения).
- Методические материалы по построению системы безопасности КИИ.
- Средства для подготовки текстовых документов (компьютер, текстовый редактор).

Ход работы

1. Изучение нормативной базы и требований

- Ознакомьтесь с основными требованиями к документации по безопасности КИИ из Федерального закона № 187-ФЗ и приказов ФСТЭК.
- Проанализируйте примеры регламентов, инструкций и положений, используемых на объектах КИИ.

2. Определение структуры и содержания документов

- Сформируйте структуру регламента по обеспечению информационной безопасности, включающую цели, задачи, обязанности, порядок контроля и отчетности.
- Разработайте инструкцию для персонала с описанием правил и процедур по обеспечению безопасности.
- Составьте положение о системе безопасности, описывающее организационную структуру, функции и взаимодействие участников системы безопасности.

3. Разработка проектов документов

- На основе анализа и требований подготовьте тексты регламента, инструкции и положения.
- Включите разделы, отражающие специфику объекта КИИ и особенности обеспечения его безопасности.

4. Обоснование выбора структуры и содержания

- Опишите, почему выбранная структура документов соответствует требованиям законодательства и специфике объекта.
- Обоснуйте включение ключевых положений и процедур.

5. Оформление отчета

- Представьте разработанные документы и обоснование их структуры и содержания.
- Дайте рекомендации по внедрению и контролю исполнения документов в организации.

Вопросы для самоконтроля

- Какие основные организационно-распорядительные документы необходимы для обеспечения информационной безопасности на объектах КИИ?
- Какие требования законодательства регулируют содержание таких документов?
- Как распределяется ответственность и полномочия в системе безопасности КИИ?
- Какие ключевые разделы должны содержать регламенты и инструкции по ИБ?
- Как обеспечить актуальность и контроль исполнения разработанных документов?

Список основной литературы

- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

- Приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении требований по обеспечению безопасности значимых объектов КИИ».
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов КИИ».
- Методические рекомендации по построению системы безопасности объектов КИИ, Мосполитех, 2022.

Список дополнительной литературы

- Документационное обеспечение процессов обеспечения безопасности значимых объектов КИИ, ЭЛВИС-ПЛЮС, 2022.
- Практическое руководство по разработке документов по информационной безопасности, Security Vision, 2023.
- Шаблоны и примеры документов по защите информации, wikisec.ru.
- Пакеты документов по информационной безопасности объектов КИИ, softagent.ru.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование

Лабораторная работа 10. Реализация мер по идентификации и аутентификации пользователей

Цель работы

Освоить практические навыки настройки и эксплуатации систем идентификации и аутентификации пользователей на объектах КИИ, а также провести анализ эффективности применяемых методов с учетом требований безопасности и нормативных актов.

Задачи

- Изучить основные методы и средства идентификации и аутентификации пользователей, применяемые на объектах КИИ.
- Настроить систему идентификации и аутентификации в тестовой среде (например, на базе ОС, серверных решений или специализированного ПО).
- Провести тестирование различных методов аутентификации (пароль, двухфакторная аутентификация, биометрия и др.).
- Оценить эффективность и надежность применяемых методов с точки зрения безопасности и удобства пользователей.
- Подготовить отчет с результатами настройки и анализа, а также рекомендациями по выбору оптимальных средств аутентификации.

Теоретическая основа

Идентификация — процесс установления личности пользователя, а аутентификация — подтверждение этой личности с помощью определенных средств (пароль, токен, биометрические данные и др.). Для объектов КИИ характерно применение многоуровневых и многофакторных методов аутентификации, что обусловлено высокими требованиями к безопасности и необходимости предотвращения несанкционированного доступа. Современные системы аутентификации включают в себя программно-аппаратные комплексы, поддерживающие различные методы, а также интеграцию с централизованными системами управления доступом.

Оборудование и материалы

- Тестовая информационная система или виртуальная среда для настройки систем аутентификации.
- Программное обеспечение для реализации различных методов аутентификации (например, Active Directory, FreeIPA, PAM-модули Linux, системы двухфакторной аутентификации).
- Документация по настройке выбранных систем.
- Методические материалы по требованиям безопасности КИИ и средствам аутентификации.

Ход работы

1. Изучение методов идентификации и аутентификации

- Ознакомьтесь с основными методами: парольная аутентификация, двухфакторная аутентификация (2FA), биометрическая аутентификация, использование смарт-карт и токенов.
- Рассмотрите требования к надежности и безопасности каждого метода в контексте КИИ.

2. Настройка системы идентификации и аутентификации

- Разверните тестовую среду (например, сервер с ОС Linux или Windows).
- Настройте базовые механизмы идентификации и аутентификации пользователей.
- Реализуйте дополнительные меры безопасности, например, 2FA с использованием приложения-генератора кодов или аппаратных токенов.
- Организуйте ведение журналов аутентификации для последующего анализа.

3. Тестирование и анализ эффективности

- Проведите тестирование различных методов аутентификации с точки зрения:
    - Надежности (устойчивость к взлому, подбору паролей).
    - Удобства для пользователей.
    - Совместимости с инфраструктурой объекта.
- Проанализируйте результаты, выявите слабые места и возможные риски.

4. Подготовка отчета

- Опишите процесс настройки и используемые методы аутентификации.
- Представьте результаты тестирования и анализа эффективности.
- Дайте рекомендации по выбору и внедрению оптимальных средств идентификации и аутентификации для объектов КИИ.

Вопросы для самоконтроля

- Какие методы идентификации и аутентификации наиболее эффективны для объектов КИИ?
- Какие преимущества и недостатки имеют различные методы аутентификации?
- Как обеспечить баланс между безопасностью и удобством пользователей?

- Какие требования предъявляются к системам аутентификации в нормативных документах по безопасности КИИ?
- Как организовать мониторинг и аудит процессов аутентификации?

Список основной литературы

- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры».
- Методические рекомендации ФСТЭК России по средствам идентификации и аутентификации на объектах КИИ, 2023.
- Учебное пособие «Обеспечение безопасности критической информационной инфраструктуры», Мосполитех, 2022.

Список дополнительной литературы

- Практическое руководство по настройке систем аутентификации, Security Vision, 2023.
- Обзор современных методов аутентификации и управления доступом, LiteraFort, 2023.
- Руководство по информационной безопасности объектов КИИ, 2022.
- Каталоги и технические описания средств аутентификации ведущих производителей.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование

Лабораторная работа 11. Управление доступом к информационным ресурсам объектов КИИ

Цель работы

Освоить методы разработки и внедрения политик управления доступом к информационным ресурсам объектов критической информационной инфраструктуры (КИИ), научиться настраивать права пользователей и организовывать контроль доступа с учетом современных требований информационной безопасности и нормативных актов.

Задачи

- Изучить основные модели и подходы к управлению доступом (ролевой, мандатный, дискреционный, на основе атрибутов).

- Разработать политику управления доступом для конкретного объекта КИИ с учетом специфики и требований безопасности.
- Настроить права доступа пользователей в тестовой системе или симуляторе с использованием выбранной модели управления доступом.
- Организовать контроль и аудит доступа, включая ведение журналов и мониторинг событий.
- Провести анализ эффективности внедренных мер и подготовить рекомендации по улучшению управления доступом.

Теоретическая основа

Управление доступом — это комплекс мер, обеспечивающих контроль использования информационных систем и ресурсов, основанный на идентификации, аутентификации и авторизации пользователей. Для объектов КИИ применяются строгие требования к разграничению прав доступа, учитывающие уровень значимости объектов и угрозы безопасности. Основные модели управления доступом включают:

- Ролевую (RBAC), где права назначаются ролям, а роли — пользователям;
- Мандатную (MAC), основанную на служебных метках конфиденциальности;
- Дискреционную (DAC), при которой доступ предоставляется владельцем ресурса;
- Управление на основе атрибутов (ABAC), где права основаны на наборе атрибутов субъектов и объектов.

Контроль доступа включает аудит, мониторинг и журналирование действий пользователей для своевременного выявления и реагирования на инциденты.

Оборудование и материалы

- Тестовая информационная система или виртуальная среда (например, Windows Server с Active Directory, Linux с PAM, специализированные симуляторы).
- Документация и методические материалы по моделям управления доступом.
- Примеры политик управления доступом и шаблоны документов.
- Инструменты для настройки прав пользователей и ведения аудита.

Ход работы

1. Изучение моделей управления доступом

- Ознакомьтесь с особенностями ролевой, мандатной, дискреционной и атрибутной моделей.
- Определите, какая модель наиболее подходит для выбранного объекта КИИ.

2. Разработка политики управления доступом

- Определите категории пользователей и их роли в организации.
- Сформулируйте правила и процедуры предоставления, изменения и отзыва прав доступа.
- Опишите меры контроля и ответственности за нарушение правил доступа.

3. Настройка прав пользователей

- Создайте учетные записи пользователей и назначьте им роли или атрибуты.
- Настройте права доступа к информационным ресурсам согласно разработанной политике.
- Организуйте многоуровневую систему прав (например, доступ к файлам, приложениям, сетевым ресурсам).

4. Организация контроля доступа

- Включите ведение журналов доступа и событий безопасности.
- Настройте мониторинг и оповещения о подозрительных действиях.
- Проведите тестирование корректности разграничения доступа.

5. Анализ эффективности и подготовка отчета

- Проанализируйте результаты настройки и контрольных мероприятий.
- Определите возможные уязвимости и риски.
- Подготовьте рекомендации по улучшению управления доступом.

Вопросы для самоконтроля

- Какие модели управления доступом существуют и чем они отличаются?
- Как разработать эффективную политику управления доступом для объекта КИИ?
- Какие инструменты используются для настройки прав пользователей?
- Как организовать контроль и аудит доступа?
- Какие нормативные требования регулируют управление доступом на объектах КИИ?

Список основной литературы

- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры».
- Методические рекомендации ФСТЭК России по управлению доступом и контролю доступа на объектах КИИ, 2023.
- Учебное пособие «Обеспечение безопасности критической информационной инфраструктуры», Мосполитех, 2022.

Список дополнительной литературы

- Руководство по управлению доступом, Security Vision, 2023.
- Практическое руководство по настройке систем управления доступом, 2022.
- Методика построения политик безопасности и контроля доступа, ФСТЭК России.
- Каталоги и описания средств управления доступом ведущих производителей.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование

Лабораторная работа 12. Организация аудита безопасности объектов КИИ

Цель работы

Освоить методы организации и проведения аудита информационной безопасности объектов критической информационной инфраструктуры (КИИ), включая сбор и анализ журналов событий, выявление инцидентов и аномалий с целью оценки текущего уровня защиты и выявления уязвимостей.

Задачи

- Изучить основные этапы и методы проведения аудита безопасности объектов КИИ.
- Ознакомиться с требованиями законодательства и нормативных документов, регламентирующих аудит ИБ на объектах КИИ.
- Провести сбор и анализ журналов событий информационных систем.
- Выявить инциденты безопасности и аномальные события на основе анализа журналов.
- Сформировать отчет с результатами аудита, выявленными уязвимостями и рекомендациями по повышению уровня безопасности.

Теоретическая основа

Аудит информационной безопасности — это независимая оценка состояния системы защиты информации объекта КИИ на соответствие нормативным требованиям и корпоративным стандартам. В рамках аудита проводится анализ технических и организационных мер, проверка эффективности систем защиты, сбор и анализ журналов безопасности для выявления инцидентов и аномалий, которые могут свидетельствовать о попытках несанкционированного доступа или других угрозах.

Важным элементом является сопоставление фактического состояния с требованиями Федерального закона № 187-ФЗ и приказов ФСТЭК России (например, № 239), а также применение практических и экспертных методов аудита.

Оборудование и материалы

- Тестовая информационная система или виртуальная среда с настроенными журналами событий.
- Инструменты для анализа журналов (например, SIEM-системы, средства просмотра и фильтрации логов).
- Нормативные документы: Федеральный закон № 187-ФЗ, Приказ ФСТЭК № 239 и методические рекомендации.
- Шаблоны отчетов и протоколов аудита.

Ход работы

1. Изучение нормативной базы и методик аудита

- Ознакомьтесь с требованиями законодательства и приказов ФСТЭК по проведению аудита ИБ на объектах КИИ.
- Изучите основные этапы аудита и методы анализа журналов событий.

2. Сбор журналов событий

- Настройте сбор журналов безопасности в тестовой системе (например, системные логи, логи сетевого оборудования, приложений).
- Обеспечьте централизованный сбор и хранение логов для удобства анализа.

3. Анализ журналов событий

- Используйте инструменты для фильтрации и поиска аномалий в журналах (например, повторяющиеся неудачные попытки входа, необычные временные промежутки активности, ошибки и предупреждения).
- Выявите события, которые могут свидетельствовать о безопасности инцидентах (взлом, попытки несанкционированного доступа, сбои).

4. Выявление инцидентов и аномалий

- Классифицируйте обнаруженные инциденты по степени критичности и типу угрозы.
- Проанализируйте возможные причины и последствия выявленных инцидентов.

5. Подготовка отчета по аудиту

- Оформите результаты анализа журналов и выявленных инцидентов.
- Включите рекомендации по устранению выявленных уязвимостей и улучшению систем мониторинга.
- Представьте план мероприятий по повышению уровня информационной безопасности объекта КИИ.

Вопросы для самоконтроля

- Какие этапы включает аудит информационной безопасности объектов КИИ?
- Какие требования законодательства регулируют проведение аудита ИБ?
- Какие типы журналов событий необходимо анализировать?
- Какие признаки аномалий и инцидентов можно выявить при анализе логов?
- Каковы основные рекомендации по улучшению безопасности на основе результатов аудита?

Список основной литературы

- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры».
- Учебное пособие «Аудит безопасности критической информационной инфраструктуры», Intelgr Publishing, 2020.
- Методические рекомендации ФСТЭК России по проведению аудита информационной безопасности объектов КИИ, 2023.

Список дополнительной литературы

- Константин Саматов, «Особенности проведения аудита информационной безопасности объектов критической информационной инфраструктуры», ITSec.ru, 2020.
- Руководство по аудиту информационной безопасности, Security Vision, 2023.
- Практическое руководство по анализу журналов безопасности и выявлению инцидентов, 2022.
- Методика аудита кибербезопасности ГИС объектов КИИ, Геосибирь, 2020.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование

Лабораторная работа 13. Реагирование на компьютерные инциденты на объектах КИИ

Цель работы
Освоить практические навыки реагирования на компьютерные инциденты (КИ) на объектах критической информационной инфраструктуры (КИИ), включая отработку сценариев реагирования, оформление необходимой отчетной документации и взаимодействие с государственной системой обнаружения и ликвидации последствий компьютерных атак (ГосСОПКА).

Задачи
- Изучить нормативные требования и методические рекомендации по реагированию на компьютерные инциденты на объектах КИИ.
- Отработать практические сценарии реагирования на различные типы инцидентов.
- Научиться оформлять отчетную документацию по инцидентам в соответствии с требованиями законодательства.
- Ознакомиться с порядком взаимодействия субъектов КИИ с ГосСОПКА и органами государственной власти.
- Разработать рекомендации по улучшению процессов реагирования и взаимодействия.

Теоретическая основа
Реагирование на компьютерные инциденты — ключевой элемент системы обеспечения информационной безопасности объектов КИИ, направленный на своевременное обнаружение, локализацию и ликвидацию последствий инцидентов. Федеральный закон № 187-ФЗ, Приказ ФСТЭК России № 239 и методические рекомендации НКЦКИ регламентируют порядок действий субъектов КИИ при обнаружении КИ, сроки информирования, состав и форму отчетной документации, а также взаимодействие с ГосСОПКА — централизованной системой мониторинга и реагирования на инциденты в критической инфраструктуре.

Оборудование и материалы
- Методические рекомендации по разработке плана реагирования на компьютерные инциденты (НКЦКИ, 2023).
- Примеры сценариев компьютерных инцидентов и шаблоны отчетных документов.
- Средства моделирования и симуляции инцидентов (виртуальная среда, специализированное ПО).
- Документация по взаимодействию с ГосСОПКА.

Ход работы
1. Изучение нормативной базы и методических рекомендаций
- Ознакомьтесь с Федеральным законом № 187-ФЗ, Приказом ФСТЭК № 239 и методическими рекомендациями НКЦКИ по реагированию на КИ.
- Изучите требования по срокам информирования и форме отчетности.
- Ознакомьтесь с функциями и структурой ГосСОПКА, порядком взаимодействия с субъектами КИИ.

2. Отработка сценариев реагирования
- Рассмотрите типовые сценарии компьютерных инцидентов (например, попытка несанкционированного доступа, распространение вредоносного ПО, отказ в обслуживании).

- Смоделируйте действия по обнаружению, локализации и ликвидации инцидента в тестовой среде или с помощью имитационных средств.
- Определите последовательность действий, ответственных лиц и сроки выполнения мероприятий.

3. Оформление отчетной документации

- Составьте отчет о компьютерном инциденте с указанием:
  - времени и способа обнаружения;
  - описания инцидента и его последствий;
  - принятых мер реагирования;
  - результатов ликвидации и восстановления.
- Подготовьте уведомление для передачи в ГосСОПКА в установленные сроки.

4. Взаимодействие с ГосСОПКА

- Ознакомьтесь с процедурами передачи информации о КИ в ГосСОПКА.
- Проанализируйте возможности автоматизации обмена данными (например, через API интеграцию SIEM-систем).
- Определите порядок взаимодействия с ведомственным или корпоративным центром ГосСОПКА.

5. Подготовка итогового отчета

- Систематизируйте результаты отработки сценариев, оформление документации и взаимодействия с ГосСОПКА.
- Дайте рекомендации по оптимизации процессов реагирования и повышения эффективности взаимодействия.

Вопросы для самоконтроля

- Какие нормативные документы регулируют реагирование на компьютерные инциденты на объектах КИИ?
- Какие основные этапы включает процесс реагирования на КИ?
- Каковы требования к отчетной документации по инцидентам?
- Как организовать взаимодействие субъекта КИИ с ГосСОПКА?
- Какие меры следует принять для минимизации последствий компьютерных инцидентов?

Список основной литературы

- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры».
- Методические рекомендации НКЦКИ по разработке плана реагирования на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак, 2023.
- ГОСТ Р 59709-2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения».

Список дополнительной литературы

- Руководство по реагированию на инциденты информационной безопасности, Security Vision, 2023.
- Практическое пособие по расследованию и ликвидации компьютерных инцидентов, Мосполитех, 2022.

- Методика управления инцидентами информационной безопасности на объектах КИИ, КиберЛенинка, 2021.
- Официальные материалы ГосСОПКА и НКЦКИ по организации взаимодействия с субъектами КИИ.

Перечень дополнительной литературы

1. Абельская, Р.Ш. Теория и практика делового общения для разработчиков программного обеспечения и IT-менеджеров : учебное пособие / Р.Ш. Абельская ; науч. ред. И. . Обабков ; Уральский федеральный университет им. первого Президента России Б. Н. Ельцина. – Екатеринбург : Издательство Уральского университета, 2018. – 113 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=275655 – Библиогр. в кн. – ISBN 978-5-7996-1215-3. – Текст : электронный.
2. Басманова, Н.И. Тренинг командообразования : учебное пособие : [16+] / Н.И. Басманова ; Технологический университет. – Москва ; Берлин : Директ-Медиа, 2019. – 60 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=572170 – Библиогр.: с. 33-34. – ISBN 978-5-4499-0549-9. – Текст : электронный.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование

Лабораторная работа 14. Применение антивирусной защиты и средств предотвращения вторжений

Цель работы

Освоить практические навыки настройки и эксплуатации антивирусных систем и систем предотвращения вторжений (IDS/IPS) на объектах КИИ, а также провести анализ их эффективности в защите информационных ресурсов от современных угроз.

Задачи

- Изучить принципы работы и основные функции антивирусных систем и IDS/IPS.
- Настроить антивирусное программное обеспечение для защиты рабочих станций и серверов.
- Развернуть и настроить систему обнаружения и предотвращения вторжений (IDS/IPS) в тестовой сети.
- Провести тестирование систем защиты с использованием имитации атак и вредоносного ПО.
- Проанализировать эффективность применяемых средств защиты и подготовить рекомендации по их оптимизации.

Теоретическая основа

Обеспечение безопасности объектов КИИ требует комплексного подхода, включающего использование антивирусных систем для обнаружения и нейтрализации вредоносных программ, а также систем предотвращения вторжений (IDS/IPS), которые мониторят сетевой трафик и события для выявления попыток несанкционированного доступа и атак. Законодательство РФ (Федеральный закон № 187-ФЗ) и нормативные документы ФСТЭК устанавливают обязательные требования к применению таких средств защиты на объектах КИИ. Эффективность этих систем зависит от корректной настройки, своевременного обновления и интеграции с другими компонентами системы безопасности.

Оборудование и материалы

- Тестовая сеть или виртуальная среда с несколькими узлами (рабочие станции, серверы).
- Антивирусное программное обеспечение (например, Dr.Web Enterprise Security Suite или аналогичные отечественные решения).
- Система IDS/IPS (например, Snort, Suricata, или коммерческие отечественные продукты).
- Инструменты для имитации атак и вредоносного ПО (тестовые вирусы, скрипты для генерации сетевого трафика).
- Документация по настройке и эксплуатации выбранных средств защиты.

Ход работы

1. Изучение функционала антивирусных систем и IDS/IPS

- Ознакомьтесь с архитектурой и основными возможностями антивирусных систем и IDS/IPS.
- Изучите требования законодательства и нормативных актов к применению этих средств на объектах КИИ.

2. Настройка антивирусной защиты

- Установите и настройте антивирусное ПО на рабочих станциях и серверах.
- Настройте регулярное обновление антивирусных баз и расписание сканирования.
- Активируйте функции контроля доступа и самозащиты антивируса.

3. Развертывание и настройка IDS/IPS

- Установите IDS/IPS-систему в тестовой сети.
- Настройте правила обнаружения и предотвращения вторжений с учетом специфики объекта КИИ.
- Организуйте сбор и анализ логов событий.

4. Тестирование и анализ эффективности

- Проведите имитацию атак (например, сканирование портов, попытки внедрения вредоносного кода, DDoS-атаки).
- Оцените реакцию антивируса и IDS/IPS на инциденты.
- Проанализируйте журналы и отчеты систем безопасности.
- Определите возможные пробелы и предложите меры по их устранению.

5. Подготовка отчета

- Опишите процесс настройки и тестирования систем защиты.
- Представьте результаты анализа эффективности.
- Дайте рекомендации по оптимизации конфигурации и интеграции средств защиты.

Вопросы для самоконтроля

- Какие функции выполняют антивирусные системы и IDS/IPS?

- Каковы особенности настройки и эксплуатации антивирусного ПО на объектах КИИ?
- Какие типы атак могут обнаруживать IDS/IPS?
- Как оценить эффективность работы средств защиты?
- Какие нормативные требования регулируют применение антивирусных и IDS/IPS-систем на объектах КИИ?

Список основной литературы

- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры».
- Методические рекомендации ФСТЭК России по применению технических средств защиты информации на объектах КИИ, 2023.
- Учебное пособие «Обеспечение безопасности критической информационной инфраструктуры», Мосполитех, 2022.

Список дополнительной литературы

- Руководство по антивирусной защите и предотвращению вторжений, Security Vision, 2023.
- Практическое руководство по настройке IDS/IPS-систем, 2022.
- Документация по Dr.Web Enterprise Security Suite и аналогичным отечественным решениям.
- Обзор современных методов защиты критической инфраструктуры от киберугроз, 2023.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

3. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
4. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

5. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
6. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
7. https://spravochnick.ru/psihologiya/ – Справочник по психологии
8. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование

Лабораторная работа 15. Обеспечение целостности и доступности информации на объектах КИИ

Цель работы

Освоить методы и средства обеспечения целостности и доступности информации на объектах критической информационной инфраструктуры (КИИ) посредством внедрения контроля целостности данных, организации резервного копирования и проведения тестирования восстановления информации после сбоев.

Задачи

- Изучить понятие целостности и доступности информации, их значение для безопасности объектов КИИ.
- Ознакомиться с методами контроля целостности данных (хэширование, цифровые подписи, контрольные суммы).
- Настроить средства контроля целостности на выбранном объекте или тестовой системе.
- Организовать процедуры резервного копирования данных и настроить автоматическое выполнение.
- Провести тестирование восстановления данных из резервных копий после имитации сбоев или потери информации.
- Оценить эффективность внедренных мер и подготовить рекомендации по их улучшению.

Теоретическая основа

Целостность информации — это свойство данных оставаться неизменными и достоверными при передаче, хранении и обработке. Контроль целостности предотвращает несанкционированные изменения и повреждения данных. Доступность информации гарантирует возможность своевременного и надежного доступа к данным при необходимости, что достигается организацией резервного копирования и восстановления. Законодательство РФ, включая Федеральный закон № 187-ФЗ и Приказ ФСТЭК № 239, требует от субъектов КИИ реализации комплексных мер по обеспечению целостности и доступности информации.

Оборудование и материалы

- Тестовая информационная система или виртуальная среда.
- Программные средства контроля целостности (например, утилиты для хэширования файлов, специализированные системы контроля).
- Средства резервного копирования (например, встроенные инструменты ОС, специализированное ПО).
- Документация по нормативным требованиям и методикам обеспечения целостности и доступности.

Ход работы

1. Изучение теоретических основ

- Ознакомьтесь с понятиями целостности и доступности информации, их ролью в безопасности КИИ.
- Изучите нормативные требования и рекомендации по контролю целостности и резервному копированию.

2. Настройка контроля целостности данных

- Выберите критичные для объекта файлы или базы данных.
- Используйте средства хэширования (например, SHA-256) для создания контрольных сумм.
- Настройте регулярную проверку целостности и уведомления о несоответствиях.

3. Организация резервного копирования

- Настройте автоматическое резервное копирование выбранных данных с учетом политики хранения.
- Определите периодичность и объем резервных копий.
- Обеспечьте хранение копий в защищенном месте.

4. Тестирование восстановления данных

- Смоделируйте ситуацию потери или повреждения данных.

- Проведите восстановление данных из резервных копий.
- Оцените полноту и скорость восстановления.

5. Анализ результатов и оформление отчета

- Опишите процесс настройки и тестирования.
- Проанализируйте эффективность контроля целостности и резервного копирования.
- Сформулируйте рекомендации по улучшению мер обеспечения целостности и доступности.

Вопросы для самоконтроля

- Что такое целостность и доступность информации и почему они важны для объектов КИИ?
- Какие методы используются для контроля целостности данных?
- Как организовать эффективное резервное копирование и восстановление данных?
- Какие нормативные требования регулируют обеспечение целостности и доступности на объектах КИИ?
- Как оценить эффективность внедренных мер защиты?

Список основной литературы

- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры».
- Кай Михайлов, Дмитрий Калинин. «Контроль целостности данных и его применение в кибербезопасности» (2024).
- ГОСТ Р 57580.1-2017 «Информационная безопасность. Процессы обеспечения безопасности информации» (раздел 7.4 — Целостность).
- Учебное пособие «Обеспечение безопасности критической информационной инфраструктуры», Мосполитех, 2022.

Список дополнительной литературы

- Руководство по обеспечению защиты и безопасности объектов КИИ, Астрал, 2023.
- Практическое руководство по резервному копированию и восстановлению данных, Security Vision, 2023.
- Методические рекомендации ФСТЭК России по контролю целостности и резервному копированию, 2023.
- Обзор современных технологий защиты информации на объектах КИИ, 2024

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии

4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование

Лабораторная работа 16. Защита технических средств и каналов передачи данных

Цель работы
Освоить практические методы и средства физической и технической защиты оборудования, а также настроить защищённые каналы передачи данных для обеспечения безопасности объектов КИИ в соответствии с нормативными требованиями.

Задачи
- Изучить основные угрозы, связанные с физическим доступом к техническим средствам и перехватом данных в каналах связи.
- Ознакомиться с мерами физической защиты оборудования (контроль доступа, охранные системы, экранирование).
- Настроить средства технической защиты (шифрование каналов, VPN, использование защищённых протоколов).
- Организовать защищённые каналы связи и проверить их работоспособность и безопасность.
- Провести анализ эффективности применённых мер защиты.
- Подготовить отчет с описанием реализованных мер и рекомендациями.

Теоретическая основа
Защита технических средств и каналов передачи данных — ключевой элемент комплексной безопасности объектов КИИ. Физическая защита предотвращает несанкционированный доступ и повреждение оборудования, а техническая защита обеспечивает конфиденциальность и целостность передаваемой информации. Согласно Приказу ФСТЭК России № 239 и Федеральному закону № 187-ФЗ, для значимых объектов КИИ применяются сертифицированные средства защиты информации, включая аппаратные и программные средства шифрования, а также меры по контролю доступа и мониторингу.

Оборудование и материалы
- Сервер или рабочая станция с сетевым оборудованием.
- Средства контроля физического доступа (например, электронные замки, системы видеонаблюдения — имитация или описание).
- Программное обеспечение для создания защищённых каналов (OpenVPN, IPsec, TLS).
- Документация по требованиям безопасности КИИ и настройке средств защиты.

Ход работы
1. Изучение угроз и мер защиты
- Ознакомьтесь с основными угрозами физической безопасности технических средств (несанкционированный доступ, кража, повреждение).
- Изучите методы защиты каналов передачи данных (шифрование, VPN, использование защищённых протоколов).

2. Организация физической защиты оборудования
- Опишите или смоделируйте меры контроля доступа к помещениям и оборудованию.
- Рассмотрите использование охранных систем, видеонаблюдения и экранирования.
- Обсудите роль организационных мер (регламенты, обучение персонала).

3. Настройка защищённых каналов передачи данных

- Разверните и настройте VPN-соединение (например, OpenVPN или IPsec) между двумя узлами.
- Настройте шифрование и аутентификацию пользователей.
- Проверьте работоспособность канала и его защищённость (например, с помощью анализа трафика).

4. Тестирование и анализ эффективности

- Проведите тестирование защищённого канала на устойчивость к перехвату и атакам.
- Оцените уровень физической защиты оборудования (по описанию или имитации).
- Сделайте выводы о соответствии применённых мер требованиям безопасности КИИ.

5. Подготовка отчета

- Опишите реализованные меры физической и технической защиты.
- Представьте результаты тестирования защищённых каналов.
- Сформулируйте рекомендации по улучшению защиты.

Вопросы для самоконтроля

- Какие угрозы существуют для технических средств и каналов передачи данных на объектах КИИ?
- Какие меры физической защиты наиболее эффективны?
- Какие технологии и протоколы применяются для защиты каналов связи?
- Как проверить эффективность настроенных средств защиты?
- Какие нормативные требования регулируют защиту технических средств и каналов передачи данных?

Список основной литературы

- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры».
- Методические рекомендации ФСТЭК России по защите технических средств и каналов передачи данных, 2023.
- Учебное пособие «Обеспечение безопасности критической информационной инфраструктуры», Мосполитех, 2022.

Список дополнительной литературы

- Обзор и практика защиты критической инфраструктуры, Security Vision, 2023.
- Практическое руководство по настройке VPN и шифрованию каналов связи, 2022.
- Руководство по физической безопасности объектов КИИ, 2023.
- Каталоги и технические описания сертифицированных средств защиты информации.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование

Лабораторная работа 17. Оценка эффективности системы обеспечения ИБ на объектах КИИ

Цель работы

Освоить методику комплексной оценки эффективности системы информационной безопасности (ИБ) на объектах критической информационной инфраструктуры (КИИ) путем проведения тестирования, анализа полученных результатов и формирования предложений по совершенствованию системы защиты.

Задачи

- Изучить нормативные требования и методики оценки состояния защиты информации на объектах КИИ, включая методику ФСТЭК по оценке показателя защищённости (КЗИ).
- Провести сбор и анализ исходных данных о состоянии системы ИБ (документы, результаты аудитов, мониторинг, опросы персонала).
- Выполнить тестирование технических и организационных мер защиты.
- Рассчитать и проанализировать показатели безопасности, включая частные показатели kji и общий коэффициент КЗИ.
- На основе анализа выявить слабые места и подготовить рекомендации по улучшению системы ИБ.
- Оформить отчет с результатами оценки и предложениями по совершенствованию.

Теоретическая основа

Методика оценки состояния защиты информации на объектах КИИ, разработанная ФСТЭК России, предусматривает определение частных показателей безопасности (kji) по группам и расчет интегрального показателя КЗИ, характеризующего степень достижения минимально необходимого уровня защиты от типовых актуальных угроз. Значение КЗИ равно 1 означает соответствие минимальным требованиям, ниже 0,75 – критический уровень, требующий немедленных мер. Оценка проводится на основе данных внутреннего контроля, внешних аудитов, мониторинга и анализа документации. Результаты служат основой для принятия управленческих решений и планирования мероприятий по повышению уровня информационной безопасности.

Оборудование и материалы

- Документы и материалы по системе ИБ объекта КИИ (политики, регламенты, результаты аудитов).
- Результаты мониторинга и журналов безопасности.

- Методические материалы ФСТЭК России по оценке состояния защиты информации (Методика оценки КЗИ).
- Инструменты для анализа данных (табличные процессоры, специализированные программы).

Ход работы

1. Подготовка и сбор исходных данных

- Запросите и изучите внутренние документы по ИБ, результаты предыдущих аудитов и мониторинга.
- Проведите опросы или интервью с ответственными сотрудниками по вопросам выполнения мер ИБ.
- Соберите данные о технических средствах защиты и их состоянии.

2. Выполнение тестирования системы ИБ

- Проведите проверку технических средств защиты (антивирусы, системы контроля доступа, шифрование и др.).
- Оцените выполнение организационных мер (обучение персонала, регламенты, процедуры).
- Зафиксируйте выявленные несоответствия и уязвимости.

3. Расчет показателей безопасности

- Определите значения частных показателей безопасности kji по группам (технические, организационные, нормативные и др.).
- Рассчитайте интегральный показатель КЗИ по формуле, учитывая весовые коэффициенты групп показателей.
- Сопоставьте результаты с нормированными значениями.

4. Анализ результатов и выявление проблем

- Проанализируйте причины снижения показателей.
- Определите приоритетные направления для улучшения системы ИБ.

5. Формирование рекомендаций

- Разработайте предложения по устранению выявленных недостатков.
- Определите мероприятия по повышению эффективности защиты информации.

6. Оформление отчета

- Подготовьте документ, включающий:
    - описание объекта и методики оценки;
    - исходные данные и результаты тестирования;
    - расчет и анализ показателей безопасности;
    - рекомендации по совершенствованию системы ИБ.

Вопросы для самоконтроля

- Какие основные показатели используются для оценки состояния защиты информации на объектах КИИ?
- Как проводится сбор и анализ исходных данных для оценки эффективности системы ИБ?
- Какие методы тестирования применяются для проверки технических и организационных мер?
- Как рассчитывается интегральный показатель КЗИ и что он означает?
- Какие мероприятия рекомендуются при выявлении низких показателей безопасности?

Список основной литературы

- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Приказ ФСТЭК России от 02 мая 2024 г. «Методика оценки текущего состояния защиты информации и обеспечения безопасности объектов КИИ».
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры».
- Учебное пособие «Обеспечение безопасности критической информационной инфраструктуры», Мосполитех, 2022.

Список дополнительной литературы

- Методика оценки технического состояния защиты информации и обеспечения безопасности объектов КИИ, ФСТЭК России, 2024.
- Руководство по аудиту и оценке информационной безопасности, Security Vision, 2023.
- Практическое руководство по управлению рисками и оценке эффективности мер ИБ, 2023.
- Обзор современных методик оценки защищённости информационных систем, 2023.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"

2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование

Лабораторная работа 18. Ознакомление с нормативно-правовой базой в области защиты КИИ

Цель работы

Изучить и проанализировать основные федеральные законы, стандарты и методики, регулирующие вопросы обеспечения безопасности критической информационной инфраструктуры в Российской Федерации, с акцентом на Федеральный закон № 187-ФЗ и соответствующие ГОСТы.

Задачи

- Ознакомиться с текстом Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Изучить основные понятия, принципы и требования, установленные в законе.
- Проанализировать нормативные документы, стандарты и методические рекомендации, применяемые в сфере защиты КИИ (в том числе ГОСТы, приказы ФСТЭК).
- Выделить ключевые обязанности субъектов КИИ и требования к обеспечению безопасности.
- Подготовить аналитический отчет с выводами и рекомендациями по применению нормативно-правовой базы в практической деятельности.

Теоретическая основа

Федеральный закон № 187-ФЗ регулирует отношения в области обеспечения безопасности КИИ, направлен на обеспечение устойчивого функционирования объектов при компьютерных атаках и иных угрозах. Закон определяет понятия КИИ, субъектов и объектов, категории значимости, порядок категорирования, обязанности владельцев и операторов, а также полномочия государственных органов. Важным дополнением являются стандарты и методики, разработанные ФСТЭК России и другими ведомствами, которые конкретизируют технические и организационные меры защиты. ГОСТы устанавливают требования к системам защиты информации и процедурам обеспечения безопасности.

Оборудование и материалы

- Тексты Федерального закона № 187-ФЗ (официальные публикации).
- Нормативные документы ФСТЭК России, включая приказы и методические рекомендации.

- ГОСТы, регламентирующие информационную безопасность (например, ГОСТ Р 57580, ГОСТ Р 50922).
- Компьютер с доступом к нормативным базам и текстовым редактором для подготовки отчета.

Ход работы

1. Изучение Федерального закона № 187-ФЗ

- Ознакомьтесь с основными положениями закона, его структурой и ключевыми статьями.
- Выделите понятия, связанные с субъектами КИИ, объектами, категориями значимости, обязанностями и полномочиями.

2. Анализ нормативных документов и стандартов

- Изучите приказы ФСТЭК России, регламентирующие обеспечение безопасности КИИ (например, Приказ № 239).
- Ознакомьтесь с основными ГОСТами, применяемыми в области ИБ КИИ.
- Проанализируйте методические рекомендации по категорированию объектов и обеспечению защиты.

3. Выделение ключевых требований и обязанностей

- Систематизируйте требования к субъектам КИИ по обеспечению безопасности.
- Определите основные меры защиты, предусмотренные нормативной базой.
- Рассмотрите порядок взаимодействия субъектов с государственными органами и ГосСОПКА.

4. Подготовка аналитического отчета

- Опишите структуру и содержание Федерального закона № 187-ФЗ.
- Представьте обзор нормативных документов и стандартов.
- Выделите ключевые обязанности и требования к субъектам КИИ.
- Сформулируйте рекомендации по применению нормативно-правовой базы в практической деятельности.

Вопросы для самоконтроля

- Каковы основные цели и задачи Федерального закона № 187-ФЗ?
- Какие субъекты и объекты относятся к критической информационной инфраструктуре?
- Какие категории значимости объектов КИИ существуют и как они определяются?
- Какие обязанности возлагаются на владельцев и операторов объектов КИИ?
- Какие нормативные документы и стандарты регулируют обеспечение безопасности КИИ?
- Как организовано взаимодействие субъектов КИИ с государственными органами?

Список основной литературы

- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»1234.
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры».
- ГОСТ Р 57580.1-2017 «Информационная безопасность. Процессы обеспечения безопасности информации».
- ГОСТ Р 50922-96 «Защита информации. Термины и определения».
- Методические рекомендации ФСТЭК России по вопросам обеспечения безопасности КИИ, 2023.

Список дополнительной литературы

- Рекомендации по реализации требований Федерального закона № 187-ФЗ, региональные семинары и материалы.
- Учебное пособие «Обеспечение безопасности критической информационной инфраструктуры», Мосполитех, 2022.
- Руководства и методики ФСТЭК России по категорированию и защите объектов КИИ.
- Обзор нормативно-правовой базы в сфере информационной безопасности, Security Vision, 2023.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование