МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«_8_» _08_____ 2023 г.

Оценка защищённости информационных систем

Методические указания по организации самостоятельной работы по дисциплине «Оценка защищённости информационных систем» для студентов направления подготовки 10.04.01 «Информационная безопасность»

Курск 2023

УДК 004.773.5

Составители: Кулешова Е.А.

Рецензент

Кандидат технических наук, доцент кафедры
вычислительной техники А.В. Киселев

Оценка защищённости информационных систем: методические указания для самостоятельной работы / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 9 с.: Библиогр.: с. 9.

Содержат сведения по вопросам самостоятельной работы на протяжении изучения дисциплины. Указывается порядок выполнения самостоятельных работ, содержание работ.

Предназначены для студентов направления подготовки 10.04.01 «Информационная безопасность».

Текст печатается в авторской редакции
Подписано в печать . Формат 60x84 1/16.
Усл. печ.л. . Уч. –изд.л. .Тираж 50 экз. Заказ .
Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Содержание самостоятельной работы

	Тема СРС	Задание
1	Нормативная база оценки защищенности ИТ	1. Исследуйте основные нормативные документы и стандарты, которые регулируют оценку защищенности информационных технологий (ИТ). 2. Объясните цели и принципы нормативной базы оценки защищенности ИТ и опишите их влияние на практику оценки и обеспечения безопасности информационных систем. 3. Выполните анализ требований, предъявляемых нормативными актами, к процессу оценки и обеспечения защищенности ИТ.
2	Основные аспекты построения системы информационной безопасности	1. Опишите основные компоненты и аспекты, которые следует учесть при построении системы информационной безопасности (СИБ). 2. Разработайте концептуальный план построения СИБ, включающий анализ угроз и рисков, разработку политик и процедур, выбор и внедрение соответствующих технических решений. 3. Проанализируйте примеры успешной реализации СИБ в организациях и оцените их эффективность.
3	Базовые вопросы проверки защищенности ИТ	1. Изучите базовые вопросы и принципы, которые следует учитывать при проверке защищенности информационных технологий. 2. Разработайте список вопросов и критериев для проверки защищенности ИТ в конкретном контексте (например, сетевая безопасность, физическая безопасность, защита данных и т. д.). 3. Создайте сценарии проверки защищенности ИТ, включающие использование предложенных вопросов и критериев.
4	Виды проверок	1. Исследуйте различные виды проверок, используемые для оценки защищенности информационных технологий в организациях. 2. Опишите сценарии и цели каждого вида проверки, таких как пенетрационное тестирование, ревизии безопасности, анализ уязвимостей и т. д. 3. Проанализируйте примеры применения каждого вида проверки в реальных ситуациях и оцените их эффективность.
5	Внутренний аудит ИБ	1. Изучите роль и задачи внутреннего аудита информационной безопасности (ИБ) в организациях. 2. Разработайте план внутреннего аудита ИБ для организации, включающий анализ процессов

		безопасности, исправление выявленных недостатков и предоставление рекомендаций по улучшению. 3. Проведите внутренний аудит ИБ в соответствии с разработанным планом и подготовьте отчет с результатами и рекомендациями.
6	Внешний аудит ИБ	1. Исследуйте роль и задачи внешнего аудита информационной безопасности (ИБ) в организациях. 2. Опишите процесс выбора и сотрудничества с внешними аудиторами ИБ, включая проведение предварительного анализа, переговоры о контракте и выполнение аудита. 3. Проанализируйте примеры проведения внешнего аудита ИБ в различных организациях и оцените его вклад в обеспечение безопасности.
7	Системы анализа защищенности	1. Изучите различные системы анализа защищенности информационных технологий и их функциональные возможности. 2. Разработайте план анализа защищенности ИТ с использование выбранной системы анализа, включая определение целей и параметров анализа, запуск анализа и интерпретацию результатов. 3. Проведите анализ защищенности ИТ с помощью выбранной системы и подготовьте отчет с результатами и рекомендациями.
8	Системы обнаружения и предотвращения вторжений	1. Исследуйте принципы и возможности систем обнаружения и предотвращения вторжений (СОПВ). 2. Разработайте план внедрения СОПВ в организации, включающий выбор подходящей системы, установку и настройку, мониторинг и реагирование на инциденты. 3. Проанализируйте примеры применения СОПВ в организациях и оцените их вклад в защиту информационных технологий от вторжений.

КОНТРОЛЬНЫЕ ВОПРОСЫ

Тема №1 «Нормативная база оценки защищенности ИТ»

1. Существующие стандарты и методологии проверки и оценки защищенности ИТ и СУИБ.
2. История развития. ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004-2011 – оценка функционирования СУИБ
3. ISO/IEC 27006:2011 и ГОСТ Р ИСО/МЭК 27006-2008 – требования к органам, осуществляющим аудит и сертификацию СУИБ.
4. ISO/IEC 27007:2011 и ISO/IEC 27008:2011 – руководства по аудиту СУИБ и средств управления ИБ, реализованных в СУИБ.
5. Существующие стандарты и методологии проверки и оценки защищенности ИТ и СУИБ: их отличия, сильные и слабые стороны.
6. ISO 19011:2002 и ГОСТ Р ИСО 19011-2003 – рекомендации по аудиту систем менеджмента качества и/или окружающей среды.
7. Какие основные нормативные документы регулируют оценку защищенности информационных технологий (ИТ)?
8. Какие критерии и методы оценки защищенности ИТ предусмотрены нормативной базой?
9. Какие организации или стандарты занимаются установлением и разработкой нормативной базы для оценки защищенности ИТ?
10. Как соотносятся между собой различные нормативные документы оценки защищенности ИТ, и какие основные различия между ними существуют?

Тема №2 «Основные аспекты построения системы информационной безопасности»

1. Назовите 3 основных аспекта построения системы информационной безопасности.
2. Административный уровень информационной безопасности. Политика безопасности информационных систем.
3. Что произойдет с организацией, если система не будет введена в эксплуатацию?
4. Программно-технические меры безопасности. Понятие сервиса информационной безопасности. Архитектурная безопасность.
5. Понятие сервиса информационной безопасности. протоколирование и аудит.
6. Понятие сервиса информационной безопасности. управление и анализ защищенности.
7. Понятие сервиса информационной безопасности. обеспечение высокой доступности и отказоустойчивости.
8. Понятие сервиса информационной безопасности. экранирование и

туннелирование.

9. Какие основные аспекты следует учесть при построении системы информационной безопасности?

10. Какие решения и меры могут быть применены для обеспечения безопасности информационных систем?

Тема №3 «Базовые вопросы проверки защищенности ИТ»

1. Назовите методы формализации процессов.
2. Назовите цели и задачи формализации процессов.
3. Важность процесса с точки зрения управления ИБ
4. Участники процесса. Связи с другими процессами СУИБ.
5. Назовите основные процессы методы проверки защищенности. Понятие процессного подхода.
6. Назовите цели и задачи процессов оценки защищенности ИТ и СУИБ.
7. Охарактеризуйте защитные оболочки и перечень преград, применяемые в учебной компьютерной лаборатории.
8. Какие основные методы контроля доступа используются в известных вам информационных системах?
9. В чем основные достоинства и недостатки методов контроля доступа?
10. Постройте неформальную модель нарушителя для учебной компьютерной лаборатории.

Тема №4 «Виды проверок»

1. Назовите внутренние аудиты ИБ.
2. Назовите внешние аудиты ИБ.
3. Мониторинг ИБ. Самооценка ИБ.
4. Как проверяется достоверность источника?
5. Гарантии безопасности компьютерных систем в системе общих критериев.
6. Проверка полномочий субъектов на доступ к ресурсам.
7. Понятие сервиса информационной безопасности. протоколирование и аудит.
8. Анализ журнала аудита ОС на рабочем месте.
9. Анализ СУИБ со стороны высшего руководства организации.
10. Перечислите виды проверок, используемые при аудите ИБ.

Тема №5 «Внутренний аудит ИБ»

1. Анализ журнала аудита ОС на рабочем месте.
2. Назовите средства и системы аудита информационной безопасности.
3. Средства администрирования сетевых программно-аппаратных комплексов защиты информации.

4. Инструментальные средства аудита безопасности компьютерных систем, их возможности и недостатки.
5. Средствами администрирования систем обнаружения компьютерных атак.
6. Методики проведения аудита информационной безопасности.
7. Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.
8. Средства автоматизации комплексного аудита информационной безопасности.
9. Методы мониторинга и аудита, выявления угроз информационной безопасности компьютерных сетей.
10. Назовите основные этапы аудита ИБ.

Тема №6 «Внешний аудит ИБ»

1. Цели и задачи, принципы проведения, управление программой, этапы проведения.
2. Аудит безопасности компьютерных систем. Цели, стандарты, подходы.
3. Компетентность аудиторов. Взаимоотношения представителей аудиторской группы и проверяемых организаций.
4. Угрозы доступности. Основные угрозы целостности. Угрозы конфиденциальности.
5. Понятие сервиса информационной безопасности. управление и анализ защищенности.
6. Понятие сервиса информационной безопасности. протоколирование и аудит.
7. Аудит прикладных служб.
8. Применение инструментальных средств аудита безопасности компьютерных систем
9. Что такое внешний аудит информационной безопасности и какова его цель?
10. Какие шаги и процедуры включает в себя проведение внешнего аудита информационной безопасности?

Тема №7 «Системы анализа защищенности»

1. Классификация защищенности компьютерной системы по требованиям безопасности информации в системе общих критериев.
2. Виды систем, решаемые задачи, использование в целях оценки защищенности ИТ.
3. Понятие сервиса информационной безопасности. управление и анализ защищенности.
4. Выявление и построение схемы информационных потоков защищаемой информации в компьютерной сети.
5. Ранжирование обнаруженных уязвимостей по степени воздействия на защищаемую информацию.

6. Разработка политик безопасности для защищенных компьютерных систем
7. Порядок сертификации средств защиты информации для разработчика СЗИ.
8. Порядок сертификации защищенных информационных систем.
9. Тестирование состояния защищенности компьютерных систем от несанкционированного доступа с использованием сканеров безопасности.
10. Какие системы анализа защищенности вы знаете?

Тема №8 «Системы обнаружения и предотвращения вторжений»

1. Назначение систем обнаружения атак. Классификация систем обнаружения атак.
2. Прямые и косвенные признаки атак. Методы обнаружения атак.
3. Сигнатурный анализ и обнаружение аномалий.
4. Классификация систем обнаружения атак (СОА).
5. Сетевые и узловые СОА.
6. Варианты размещения СОА.
7. Размещение сенсоров СОА.
8. Требования, предъявляемые к СОА.
9. Стандартизация в области обнаружения атак. Архитектура СОА.
10. Система определения маршрутов прохождения сетевых пакетов, обнаружения объектов сети, построения схемы сети.

ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННЫХ РЕСУРСОВ

1. Технологии обеспечения безопасности информационных систем : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.

2. Основы администрирования информационных систем : учебное пособие / Д. О. Бобынцев, А. Л. Марухленко, Л. О. Марухленко [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 202 с. – URL: https://biblioclub.ru/index.php?page=book&id=598955 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.

3. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 255 с. – URL: https://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 28.02.2023). – Режим доступа: по подписке. – Текст : электронный.

4. Спицын, В. Г. Информационная безопасность вычислительной техники : учебное пособие / В. Г. Спицын ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Эль Контент, 2011. – 148 с. – URL: https://biblioclub.ru/index.php?page=book&id=208694 (дата обращения: 28.02.2023). – Режим доступа: по подписке. – Текст : электронный.

5. Системы защиты информации в ведущих зарубежных странах : учебное пособие / В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский ; науч. ред. В. И. Аверченков. – 5-е изд., стер. – Москва : ФЛИНТА, 2021. – 224 с. – URL: https://biblioclub.ru/index.php?page=book&id=93351 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.