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

Методические указания

по выполнению практических работ
по дисциплине
«МЕНЕДЖМЕНТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ»
для студентов направления подготовки
02.04.01 Математика и компьютерные науки
профиль «Искусственный интеллект в кибербезопасности»

Ставрополь
2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 3
СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ 5
Практическое занятие 1. Настройка и использование SIEM-системы для обнаружения инцидентов. 5
Практическое занятие 2. Анализ логов безопасности и выявление аномальной активности. 6
Практическое занятие 3. Расследование инцидента утечки данных с использованием инструментов судебной экспертизы. 7
Практическое занятие 4. Реагирование на DDoS-атаку: методология и практические меры. 9
Практическое занятие 5. Обнаружение и анализ вредоносного ПО в корпоративной сети. 10
Практическое занятие 6. Работа с фишинговыми атаками: выявление, анализ и реагирование. 12
Практическое занятие 7. Исследование инцидента компрометации учетных данных. 13
Практическое занятие 8. Практическое применение сценариев реагирования на инциденты в SOC. 15
Практическое занятие 9. Пост-инцидентный анализ и разработка отчета о расследовании. 16
Практическое занятие 10. Разработка и тестирование плана реагирования на кибератаки. 18

ВВЕДЕНИЕ

Цель и задачи освоения дисциплины

Целью освоения дисциплины «Менеджмент инцидентов информационной безопасности информационных систем» является формирование у будущего специалиста по направлению подготовки 02.04.01 Математика и компьютерные науки профиль «Искусственный интеллект в кибербезопасности» понимания основных методов, реализации успешной командной работы, применение ИТ-технологий для эффективного взаимодействия в команде и развития проектной деятельности.

Задачи дисциплины:

- Дисциплина призвана содействовать усилению практической направленности образования, формированию и укреплению технической, нормативнометодической культуры студентов

Перечень осваиваемых компетенций:

Код	Формулировка
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы высшего образования

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций, индикаторов
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	**ИД-1** Формулирует цель проекта, определяет совокупность взаимосвязанных задач, обеспечивающих ее достижение и определяет ожидаемые результаты решения задач.	Формулирует цель проекта, создает паспорт проекта
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать	**ИД-2** Разрабатывает план действий для решения задач проекта, выбирая оптимальный способ их решения, исходя из	Разрабатывает план действий по управлению проектом на всех этапах его жизненного цикла,

оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	действующих правовых норм и имеющихся ресурсов и ограничений	создает портфолио проекта

СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Практическое занятие 1. Настройка и использование SIEM-системы для обнаружения инцидентов.

Цель работы:
Ознакомить студентов с принципами работы SIEM-систем и их ролью в обнаружении инцидентов информационной безопасности. Практическое применение SIEM для мониторинга и анализа событий безопасности.

Задачи:

1. **Изучение функциональных возможностей SIEM-систем**:
   - Ознакомиться с основными компонентами SIEM: сбор данных, предварительная обработка, хранение, анализ и представление.
   - Понять роль корреляции событий в обнаружении угроз.
2. **Настройка SIEM-системы**:
   - Выбрать open-source решение для SIEM (например, ELK Stack или OSSEC).
   - Настроить сбор логов с различных источников (серверы, рабочие станции, сетевые устройства).
   - Конфигурировать правила корреляции для обнаружения типичных инцидентов ИБ (например, атаки типа «перебор пароля»).
3. **Симуляция инцидентов**:
   - Создать сценарий атаки (например, перебор пароля или попытка несанкционированного доступа).
   - Запустить симуляцию и отслеживать реакцию SIEM-системы.
4. **Анализ результатов**:
   - Проанализировать отчеты и оповещения, сгенерированные SIEM-системой.
   - Оценить эффективность системы в обнаружении и реагировании на инциденты.
5. **Отчетность**:
   - Составить отчет о проведенной работе, включая:
     - Описание настроенной SIEM-системы.
     - Описание симулированных инцидентов.
     - Анализ результатов и выводы о эффективности SIEM-системы.

Инструменты и ресурсы:

- **Open-source решения для SIEM**: ELK Stack (Elasticsearch, Logstash, Kibana), OSSEC.
- **Симуляторы атак**: Nmap, Metasploit (для симуляции атак).
- **Документация и учебные материалы**: Positive Technologies, CISOCLUB.

Перечень основной литературы

1. Поздняк, И. С. Управление информационной безопасностью : методические указания / И. С. Поздняк, И. С. Макаров. — Самара : ПГУТИ, 2020. — 43 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223313
2. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. — Йошкар-Ола : ПГТУ, 2020. — 154 с. — ISBN 978-

5-8158-2165-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157473

Перечень дополнительной литературы

1. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – 3-е изд. – Москва : РИОР : ИНФРА-М, 2021. –400 с. – (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. Документ подписан простой электронной подписью Информация о владельце: ФИО: Петренко Вячеслав Иванович Должность: и.о. директора Института цифрового развития Дата подписания: 27.03.2024 16:03:15 Уникальный программный ключ: b47f96eea65a16e179f94dbf7fb0b10000e7ad4d
2. Астахов, А.М. Искусство управления информационными рисками [Электронный ресурс] / А.М. Астахов. – М. : ДМК Пресс, 2010. – 312 с. - ISBN 978-5-94074-574-7. - URL: http://biblioclub.ru/index.php? page=book&id=86481
3. Анисимов, А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. – М. : Интернет-Университет Информационных Технологий, 2009. - 176 с. - ISBN 9778-5-9963-0237-6. - URL: http://biblioclub.ru/index.php?page=book&id=232981

Практическое занятие 2. Анализ логов безопасности и выявление аномальной активности.

Цель работы:

Ознакомить студентов с методами анализа логов безопасности для выявления аномальной активности и инцидентов информационной безопасности.

Задачи:

1. **Изучение источников логов**:
   - Ознакомиться с основными источниками логов безопасности: журналы операционных систем (Windows/Linux), журналы приложений (веб-сервер, база данных), журналы сетевых устройств (syslog) и инструментов безопасности (Sysmon, OSSEC).
2. **Анализ логов**:
   - Использовать чек-лист для анализа логов безопасности, включая:
     - **Определение источников журналов** и автоматизированных инструментов для анализа.
     - **Сбор и обработка логов** в одном месте.
     - **Создание правил** для уменьшения «зашумленности» логов.
     - **Анализ меток времени** и учёт часовых поясов.
     - **Выявление необычных событий**: последние изменения, сбои, ошибки, доступ и т.п..
   - Применить команды для анализа логов в Linux: cat, zcat, bzcat, grep.
3. **Выявление аномальной активности**:
   - **Симуляция инцидентов**: попытки несанкционированного доступа, перебор пароля или атаки на веб-сервер.
   - **Анализ логов** для обнаружения симулированных инцидентов.
   - **Оценка эффективности** выявления аномальной активности.
4. **Отчетность**:
   - Составить отчет о проведенной работе, включая:

- Описание источников логов и инструментов, использованных для анализа.
- Описание симулированных инцидентов и методов их обнаружения.
- Анализ результатов и выводы о эффективности анализа логов.

Инструменты и ресурсы:

- **Инструменты для анализа логов**: ELK Stack, Sysmon, OSSEC.
- **Симуляторы атак**: Nmap, Metasploit.
- **Документация и учебные материалы**: Positive Technologies, CISOCLUB.

Перечень основной литературы

1. Поздняк, И. С. Управление информационной безопасностью : методические указания / И. С. Поздняк, И. С. Макаров. — Самара : ПГУТИ, 2020. — 43 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223313
2. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. — Йошкар-Ола : ПГТУ, 2020. — 154 с. — ISBN 978-5-8158-2165-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157473

Перечень дополнительной литературы

1. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – 3-е изд. – Москва : РИОР : ИНФРА-М, 2021. –400 с. – (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. Документ подписан простой электронной подписью Информация о владельце: ФИО: Петренко Вячеслав Иванович Должность: и.о. директора Института цифрового развития Дата подписания: 27.03.2024 16:03:15 Уникальный программный ключ: b47f96eea65a16e179f94dbf7fb0b10000e7ad4d
2. Астахов, А.М. Искусство управления информационными рисками [Электронный ресурс] / А.М. Астахов. – М. : ДМК Пресс, 2010. – 312 с. - ISBN 978-5-94074-574-7. - URL: http://biblioclub.ru/index.php? page=book&id=86481
3. Анисимов, А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. – М. : Интернет-Университет Информационных Технологий, 2009. - 176 с. - ISBN 9778-5-9963-0237-6. - URL: http://biblioclub.ru/index.php?page=book&id=232981

Практическое занятие 3. Расследование инцидента утечки данных с использованием инструментов судебной экспертизы.

Цель работы:

Ознакомить студентов с методами расследования утечек данных, используя инструменты судебной экспертизы, и практическим применением этих методов для выявления причин и последствий утечек.

Задачи:

1. **Изучение теоретических основ**:
    - Ознакомиться с основными видами утечек данных (например, через сотрудников, взлом, уязвимости в ПО) и их последствиями.

- Понять роль судебной компьютерной экспертизы в расследовании утечек данных.

2. **Симуляция утечки данных**:
   - Создать сценарий утечки данных (например, через фотографирование экрана или несанкционированный доступ к базе данных).
   - Симулировать утечку и фиксировать все действия и события.
3. **Сбор доказательств**:
   - Использовать инструменты для сбора логов и данных о событиях безопасности (например, Sysmon, OSSEC).
   - Собрать информацию о системных настройках и конфигурациях на момент инцидента.
4. **Анализ инцидента**:
   - Проанализировать собранные данные для выявления причин и масштабов утечки.
   - Использовать инструменты судебной экспертизы для восстановления хода событий и определения виновных лиц.
5. **Подготовка отчета**:
   - Составить отчет о проведенном расследовании, включая:
     - Описание симулированного инцидента.
     - Методы сбора и анализа доказательств.
     - Выводы о причинах утечки и рекомендации по предотвращению подобных инцидентов в будущем.

Инструменты и ресурсы:

- **Инструменты судебной экспертизы**: Sysmon, OSSEC, инструменты для анализа логов (ELK Stack).
- **Симуляторы атак**: Nmap, Metasploit.
- **Документация и учебные материалы**: Positive Technologies, CISOCLUB.

Перечень основной литературы

1. Поздняк, И. С. Управление информационной безопасностью : методические указания / И. С. Поздняк, И. С. Макаров. — Самара : ПГУТИ, 2020. — 43 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223313
2. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. — Йошкар-Ола : ПГТУ, 2020. — 154 с. — ISBN 978-5-8158-2165-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157473

Перечень дополнительной литературы

1. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – 3-е изд. – Москва : РИОР : ИНФРА-М, 2021. –400 с. – (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. Документ подписан простой электронной подписью Информация о владельце: ФИО: Петренко Вячеслав Иванович Должность: и.о. директора Института цифрового развития Дата подписания: 27.03.2024 16:03:15 Уникальный программный ключ: b47f96eea65a16e179f94dbf7fb0b10000e7ad4d

2. Астахов, А.М. Искусство управления информационными рисками [Электронный ресурс] / А.М. Астахов. – М. : ДМК Пресс, 2010. – 312 с. - ISBN 978-5-94074-574-7. - URL: http://biblioclub.ru/index.php? page=book&id=86481
3. Анисимов, А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. – М. : Интернет-Университет Информационных Технологий, 2009. - 176 с. - ISBN 9778-5-9963-0237-6. - URL: http://biblioclub.ru/index.php?page=book&id=232981

Практическое занятие 4. Реагирование на DDoS-атаку: методология и практические меры.

Цель работы:
Ознакомить студентов с методологией реагирования на DDoS-атаки и практическими мерами по их предотвращению и смягчению последствий.

Задачи:

1. **Изучение теоретических основ**:
   - Ознакомиться с видами DDoS-атак и их последствиями для IT-инфраструктуры.
   - Понять роль мониторинга и анализа трафика в обнаружении атак.
2. **Симуляция DDoS-атаки**:
   - Использовать инструменты для симуляции DDoS-атаки (например, Apache JMeter или Nmap).
   - Запустить симуляцию и отслеживать реакцию системы.
3. **Немедленные действия при обнаружении атаки**:
   - **Анализ источника трафика**: определение IP-адресов или регионов, из которых поступает вредоносный трафик.
   - **Активация защитных механизмов**: включение веб-аппликационных файерволлов (WAF) и других защитных инструментов.
   - **Связь с провайдером**: уведомление интернет-провайдера для получения дополнительных мер защиты.
   - **Ограничение доступа**: временное ограничение доступа из определенных IP-адресов или регионов.
4. **Практические меры по смягчению последствий**:
   - **Перенаправление трафика**: использование DNS или CDN для распределения нагрузки.
   - **Фильтрация трафика**: применение алгоритмов распознавания образов для блокировки вредоносных пакетов.
   - **Настройка резервных ресурсов**: использование резервных серверов и сетевых маршрутов для поддержания доступности услуг.
5. **Отчетность**:
   - Составить отчет о проведенной работе, включая:
     - Описание симулированной DDoS-атаки.
     - Методы обнаружения и реагирования.
     - Выводы о эффективности примененных мер и рекомендации по улучшению защиты.

Инструменты и ресурсы:

- **Инструменты для симуляции DDoS**: Apache JMeter, Nmap.

- **Защитные инструменты**: WAF, DNS, CDN.
- **Документация и учебные материалы**: Selectel, Skypro, Security Vision.

Перечень основной литературы

1. Поздняк, И. С. Управление информационной безопасностью : методические указания / И. С. Поздняк, И. С. Макаров. — Самара : ПГУТИ, 2020. — 43 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223313

2. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. — Йошкар-Ола : ПГТУ, 2020. — 154 с. — ISBN 978-5-8158-2165-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157473

Перечень дополнительной литературы

1. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – 3-е изд. – Москва : РИОР : ИНФРА-М, 2021. –400 с. – (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. Документ подписан простой электронной подписью Информация о владельце: ФИО: Петренко Вячеслав Иванович Должность: и.о. директора Института цифрового развития Дата подписания: 27.03.2024 16:03:15 Уникальный программный ключ: b47f96eea65a16e179f94dbf7fb0b10000e7ad4d

2. Астахов, А.М. Искусство управления информационными рисками [Электронный ресурс] / А.М. Астахов. – М. : ДМК Пресс, 2010. – 312 с. - ISBN 978-5-94074-574-7. - URL: http://biblioclub.ru/index.php? page=book&id=86481

3. Анисимов, А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. – М. : Интернет-Университет Информационных Технологий, 2009. - 176 с. - ISBN 9778-5-9963-0237-6. - URL: http://biblioclub.ru/index.php?page=book&id=232981

Практическое занятие 5. Обнаружение и анализ вредоносного ПО в корпоративной сети.

Цель работы:
Ознакомить студентов с методами обнаружения и анализа вредоносного ПО в корпоративной сети, а также с практическими мерами по их предотвращению и смягчению последствий.

Задачи:
1. **Изучение теоретических основ**:
    - Ознакомиться с видами вредоносного ПО (вирусы, трояны, эксплойты) и их распространением (фишинговые атаки, зараженные веб-сайты).
    - Понять роль сетевых и конечных устройств в обнаружении вредоносного ПО.
2. **Симуляция заражения вредоносным ПО**:

- Использовать симуляторы вредоносного ПО или тестовые образцы (например, EICAR) для моделирования заражения.
- Запустить симуляцию и отслеживать реакцию системы.

3. **Анализ сетевого трафика**:
   - Использовать инструменты анализа сетевого трафика (NTA) для выявления аномалий, связанных с вредоносным ПО.
   - Проанализировать сетевые протоколы и порты для обнаружения подозрительной активности.
4. **Использование систем обнаружения вторжений (IDS)**:
   - Настроить IDS для обнаружения вредоносного трафика и генерации оповещений.
   - Оценить эффективность IDS в выявлении симулированного вредоносного ПО.
5. **Практические меры по смягчению последствий**:
   - **Изоляция зараженных устройств**: временная изоляция устройств, на которых обнаружено вредоносное ПО.
   - **Обновление антивирусного ПО**: актуализация баз данных антивирусных программ для обнаружения новых угроз.
   - **Оркестровка действий**: автоматизация предопределенных действий в ответ на обнаружение вредоносного ПО.
6. **Отчетность**:
   - Составить отчет о проведенной работе, включая:
     - Описание симулированного заражения.
     - Методы обнаружения и анализа вредоносного ПО.
     - Выводы о эффективности примененных мер и рекомендации по улучшению защиты.

Инструменты и ресурсы:

- **Инструменты анализа сетевого трафика**: PT NAD, Cisco Stealthwatch.
- **Системы обнаружения вторжений**: IDS, SIEM.
- **Симуляторы вредоносного ПО**: EICAR.
- **Документация и учебные материалы**: Positive Technologies, Kaspersky.

Перечень основной литературы

1. Поздняк, И. С. Управление информационной безопасностью : методические указания / И. С. Поздняк, И. С. Макаров. — Самара : ПГУТИ, 2020. — 43 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223313
2. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. — Йошкар-Ола : ПГТУ, 2020. — 154 с. — ISBN 978-5-8158-2165-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157473

Перечень дополнительной литературы

1. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – 3-е изд. – Москва : РИОР : ИНФРА-М, 2021. –400 с. – (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. Документ подписан простой электронной подписью Информация о владельце: ФИО: Петренко Вячеслав Иванович Должность: и.о.

директора Института цифрового развития Дата подписания: 27.03.2024 16:03:15 Уникальный программный ключ: b47f96eea65a16e179f94dbf7fb0b10000e7ad4d
2. Астахов, А.М. Искусство управления информационными рисками [Электронный ресурс] / А.М. Астахов. – М. : ДМК Пресс, 2010. – 312 с. - ISBN 978-5-94074-574-7. - URL: http://biblioclub.ru/index.php? page=book&id=86481
3. Анисимов, А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. – М. : Интернет-Университет Информационных Технологий, 2009. - 176 с. - ISBN 9778-5-9963-0237-6. - URL: http://biblioclub.ru/index.php?page=book&id=232981

Практическое занятие 6. Работа с фишинговыми атаками: выявление, анализ и реагирование.

Цель работы:
Ознакомить студентов с методами выявления, анализа и реагирования на фишинговые атаки, а также с практическими мерами по их предотвращению.

Задачи:
1. **Изучение теоретических основ**:
   - Ознакомиться с видами фишинговых атак: **обычный фишинг**, **целевой фишинг (spear phishing)**, **уэйлинг (whaling)**, **смишинг (smishing)**, **вишинг (vishing)**.
   - Понять роль социальной инженерии в фишинговых атаках.
2. **Симуляция фишинговых атак**:
   - Создать сценарий фишинговой атаки (например, целевой фишинг на сотрудника компании).
   - Симулировать отправку фишинговых писем и отслеживать реакцию системы.
3. **Анализ фишинговых писем**:
   - Использовать инструменты для анализа электронных писем (например, проверка домена отправителя, содержимого и ссылок).
   - Определить признаки фишинга: орфографические ошибки, подозрительные ссылки, нестандартные просьбы.
4. **Практические меры по предотвращению и реагированию**:
   - **Обучение сотрудников**: проведение семинаров по распознаванию фишинговых писем.
   - **Настройка фильтров**: использование антивирусного ПО и фильтров электронной почты для блокировки подозрительных писем.
   - **Создание протокола реагирования**: разработка плана действий в случае обнаружения фишинговой атаки.
5. **Отчетность**:
   - Составить отчет о проведенной работе, включая:
     - Описание симулированной фишинговой атаки.
     - Методы анализа и выявления фишинга.
     - Выводы о эффективности примененных мер и рекомендации по улучшению защиты.

Инструменты и ресурсы:
- **Инструменты анализа электронной почты**: антивирусное ПО с функцией фильтрации спама.
- **Симуляторы фишинговых атак**: тестовые образцы фишинговых писем.
- **Документация и учебные материалы**: Kaspersky, Trend Micro.

Перечень основной литературы

1. Поздняк, И. С. Управление информационной безопасностью : методические указания / И. С. Поздняк, И. С. Макаров. — Самара : ПГУТИ, 2020. — 43 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223313
2. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. — Йошкар-Ола : ПГТУ, 2020. — 154 с. — ISBN 978-5-8158-2165-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157473

Перечень дополнительной литературы

1. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – 3-е изд. – Москва : РИОР : ИНФРА-М, 2021. –400 с. – (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. Документ подписан простой электронной подписью Информация о владельце: ФИО: Петренко Вячеслав Иванович Должность: и.о. директора Института цифрового развития Дата подписания: 27.03.2024 16:03:15 Уникальный программный ключ: b47f96eea65a16e179f94dbf7fb0b10000e7ad4d
2. Астахов, А.М. Искусство управления информационными рисками [Электронный ресурс] / А.М. Астахов. – М. : ДМК Пресс, 2010. – 312 с. - ISBN 978-5-94074-574-7. - URL: http://biblioclub.ru/index.php? page=book&id=86481
3. Анисимов, А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. – М. : Интернет-Университет Информационных Технологий, 2009. - 176 с. - ISBN 9778-5-9963-0237-6. - URL: http://biblioclub.ru/index.php?page=book&id=232981

Практическое занятие 7. Исследование инцидента компрометации учетных данных.

Цель работы:

Ознакомить студентов с методами исследования инцидентов компрометации учетных данных, а также с практическими мерами по их предотвращению и смягчению последствий.

Задачи:

1. **Изучение теоретических основ**:
    - Ознакомиться с видами атак на учетные данные: **кража учетных данных, атаки типа Pass-the-Hash (PtH), атаки типа Pass-the-Ticket (PtT)**.

- Понять роль учетных записей с высоким уровнем привилегий в компрометации систем.

2. **Симуляция компрометации учетных данных**:
    - Использовать инструменты для симуляции атак на учетные данные (например, PtH с помощью утилит для работы с хэшами паролей).
    - Запустить симуляцию и отслеживать реакцию системы.
3. **Анализ инцидента**:
    - Проанализировать журналы безопасности для выявления признаков компрометации.
    - Использовать инструменты для анализа сетевого трафика для обнаружения подозрительной активности.
4. **Практические меры по предотвращению и смягчению последствий**:
    - **Использование MFA**: настройка многофакторной аутентификации для повышения безопасности входа.
    - **Управление привилегиями**: ограничение привилегий учетных записей и использование отдельных административных учетных записей.
    - **Регулярные аудиты**: проведение регулярных аудитов безопасности для выявления уязвимостей.
5. **Отчетность**:
    - Составить отчет о проведенной работе, включая:
        - Описание симулированного инцидента компрометации.
        - Методы анализа и выявления компрометации.
        - Выводы о эффективности примененных мер и рекомендации по улучшению защиты.

Инструменты и ресурсы:

- **Инструменты для симуляции атак**: утилиты для работы с хэшами паролей (например, Mimikatz).
- **Системы обнаружения вторжений**: IDS, SIEM.
- **Документация и учебные материалы**: Microsoft Learn, Positive Technologies.

Перечень основной литературы

1. Поздняк, И. С. Управление информационной безопасностью : методические указания / И. С. Поздняк, И. С. Макаров. — Самара : ПГУТИ, 2020. — 43 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223313
2. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. — Йошкар-Ола : ПГТУ, 2020. — 154 с. — ISBN 978-5-8158-2165-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157473

Перечень дополнительной литературы

1. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – 3-е изд. – Москва : РИОР : ИНФРА-М, 2021. –400 с. – (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. Документ подписан простой электронной подписью Информация о владельце: ФИО: Петренко Вячеслав Иванович Должность: и.о. директора Института цифрового развития Дата подписания: 27.03.2024 16:03:15 Уникальный программный ключ: b47f96eea65a16e179f94dbf7fb0b10000e7ad4d
2. Астахов, А.М. Искусство управления информационными рисками [Электронный ресурс] / А.М. Астахов. – М. : ДМК Пресс, 2010. – 312 с. - ISBN 978-5-94074-574-7. - URL: http://biblioclub.ru/index.php? page=book&id=86481
3. Анисимов, А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. – М. : Интернет-Университет Информационных Технологий, 2009. - 176 с. - ISBN 9778-5-9963-0237-6. - URL: http://biblioclub.ru/index.php?page=book&id=232981

Практическое занятие 8. Практическое применение сценариев реагирования на инциденты в SOC.

Цель работы:

Ознакомить студентов с практическим применением сценариев реагирования на инциденты в Центре мониторинга и реагирования на инциденты безопасности (SOC) и развить навыки в разработке и использовании плейбуков для различных типов угроз.

Задачи:

1. **Изучение теоретических основ**:
   - Ознакомиться с ролью SOC в обнаружении и реагировании на инциденты безопасности.
   - Понять важность плейбуков в реагировании на инциденты.
2. **Разработка плейбуков**:
   - Создать плейбуки для следующих сценариев:
     - **Утечка данных**: выявление источника утечки и блокировка доступа к скомпрометированным данным.
     - **Фишинговая атака**: выявление и блокировка вредоносных писем, обучение сотрудников.
     - **Вредоносное ПО**: изоляция зараженных устройств и удаление вредоносного ПО.
3. **Симуляция инцидентов**:
   - Использовать симуляторы или тестовые сценарии для моделирования инцидентов (например, утечка данных, фишинговая атака).
   - Применить разработанные плейбуки для реагирования на симулированные инциденты.
4. **Анализ эффективности**:
   - Оценить эффективность плейбуков в реагировании на инциденты.
   - Проанализировать время реагирования и масштабы ущерба.
5. **Отчетность**:

- Составить отчет о проведенной работе, включая:
    - Описание разработанных плейбуков.
    - Методы симуляции и реагирования на инциденты.
    - Выводы о эффективности плейбуков и рекомендации по улучшению.

Инструменты и ресурсы:

- **Инструменты для симуляции инцидентов**: Nmap, Metasploit.
- **Системы управления событиями безопасности (SIEM)**: ELK Stack, Splunk.
- **Документация и учебные материалы**: Microsoft Learn, Kaspersky Labs.

Перечень основной литературы

1. Поздняк, И. С. Управление информационной безопасностью : методические указания / И. С. Поздняк, И. С. Макаров. — Самара : ПГУТИ, 2020. — 43 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223313

2. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. — Йошкар-Ола : ПГТУ, 2020. — 154 с. — ISBN 978-5-8158-2165-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157473

Перечень дополнительной литературы

1. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – 3-е изд. – Москва : РИОР : ИНФРА-М, 2021. –400 с. – (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. Документ подписан простой электронной подписью Информация о владельце: ФИО: Петренко Вячеслав Иванович Должность: и.о. директора Института цифрового развития Дата подписания: 27.03.2024 16:03:15 Уникальный программный ключ: b47f96eea65a16e179f94dbf7fb0b10000e7ad4d

2. Астахов, А.М. Искусство управления информационными рисками [Электронный ресурс] / А.М. Астахов. – М. : ДМК Пресс, 2010. – 312 с. - ISBN 978-5-94074-574-7. - URL: http://biblioclub.ru/index.php? page=book&id=86481

3. Анисимов, А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. – М. : Интернет-Университет Информационных Технологий, 2009. - 176 с. - ISBN 9778-5-9963-0237-6. - URL: http://biblioclub.ru/index.php?page=book&id=232981

Практическое занятие 9. Пост-инцидентный анализ и разработка отчета о расследовании.

Цель работы:

Ознакомить студентов с методами пост-инцидентного анализа и разработкой отчетов о расследовании инцидентов информационной безопасности, а также с практическими мерами по улучшению безопасности на основе результатов анализа.

Задачи:

1. **Изучение теоретических основ**:
   - Ознакомиться с этапами пост-инцидентного анализа: определение причин инцидента, оценка воздействия, выявление сильных и слабых сторон системы безопасности.
   - Понять важность документирования инцидентов и разработки отчетов для улучшения безопасности.
2. **Симуляция инцидента**:
   - Использовать симуляторы или тестовые сценарии для моделирования инцидента (например, утечка данных или атака вредоносным ПО).
   - Запустить симуляцию и отслеживать реакцию системы.
3. **Пост-инцидентный анализ**:
   - Проанализировать журналы безопасности, сетевой трафик и системные данные для понимания хода событий и масштабов инцидента.
   - Оценить эффективность мер реагирования и выявить области для улучшения.
4. **Разработка отчета**:
   - Составить отчет о расследовании инцидента, включая:
     - Описание инцидента и его последствий.
     - Анализ причин и факторов, способствовавших инциденту.
     - Оценка эффективности мер реагирования.
     - Рекомендации по улучшению безопасности и предотвращению подобных инцидентов в будущем.
5. **Представление результатов**:
   - Презентовать отчет команде или руководству, обсуждая выводы и рекомендации.

Инструменты и ресурсы:

- **Инструменты для симуляции инцидентов**: Nmap, Metasploit.
- **Системы управления событиями безопасности (SIEM)**: ELK Stack, Splunk.
- **Документация и учебные материалы**: NIST SP 800-61, CISOCLUB.

Перечень основной литературы

1. Поздняк, И. С. Управление информационной безопасностью : методические указания / И. С. Поздняк, И. С. Макаров. — Самара : ПГУТИ, 2020. — 43 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223313
2. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. — Йошкар-Ола : ПГТУ, 2020. — 154 с. — ISBN 978-5-8158-2165-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157473

Перечень дополнительной литературы

1. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – 3-е изд. – Москва : РИОР : ИНФРА-М, 2021. –400 с. – (Высшее образование). — DOI:

https://doi.org/10.12737/1759-3. Документ подписан простой электронной подписью Информация о владельце: ФИО: Петренко Вячеслав Иванович Должность: и.о. директора Института цифрового развития Дата подписания: 27.03.2024 16:03:15 Уникальный программный ключ: b47f96eea65a16e179f94dbf7fb0b10000e7ad4d
2. Астахов, А.М. Искусство управления информационными рисками [Электронный ресурс] / А.М. Астахов. – М. : ДМК Пресс, 2010. – 312 с. - ISBN 978-5-94074-574-7. - URL: http://biblioclub.ru/index.php? page=book&id=86481
3. Анисимов, А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. – М. : Интернет-Университет Информационных Технологий, 2009. - 176 с. - ISBN 9778-5-9963-0237-6. - URL: http://biblioclub.ru/index.php?page=book&id=232981

Практическое занятие 10. Разработка и тестирование плана реагирования на кибератаки.

Цель работы:
Ознакомить студентов с методами разработки и тестирования планов реагирования на кибератаки, а также с практическими мерами по их реализации и оценке эффективности.

Задачи:
1. **Изучение теоретических основ**:
   - Ознакомиться с основными видами кибератак (DDoS, фишинг, вредоносное ПО) и их последствиями для бизнеса.
   - Понять роль плана реагирования в минимизации ущерба от кибератак.
2. **Разработка плана реагирования**:
   - Создать план реагирования на кибератаки, включая:
     - **Оценку рисков**: определение критически важных активов и потенциальных угроз.
     - **Формирование команды реагирования**: назначение ролей и обязанностей.
     - **Разработка сценариев реагирования**: создание блок-схем для различных типов атак.
     - **Внедрение систем мониторинга и резервного копирования**: использование SIEM и резервного копирования для быстрого восстановления.
3. **Симуляция кибератак**:
   - Использовать инструменты для симуляции кибератак (например, Nmap, Metasploit).
   - Запустить симуляцию и отслеживать реакцию системы.
4. **Тестирование плана реагирования**:
   - Применить разработанный план для реагирования на симулированные атаки.
   - Оценить эффективность плана в сдерживании и восстановлении после атак.
5. **Анализ результатов**:
   - Проанализировать время реагирования, масштабы ущерба и эффективность мер по восстановлению.
   - Выявить области для улучшения и доработки плана.
6. **Отчетность**:
   - Составить отчет о проведенной работе, включая:

- Описание разработанного плана реагирования.
- Методы симуляции и тестирования.
- Выводы о эффективности плана и рекомендации по улучшению.

Инструменты и ресурсы:

- **Инструменты для симуляции атак**: Nmap, Metasploit.
- **Системы управления событиями безопасности (SIEM)**: ELK Stack, Splunk.
- **Документация и учебные материалы**: Microsoft Learn, Positive Technologies.

Перечень основной литературы

1. Поздняк, И. С. Управление информационной безопасностью : методические указания / И. С. Поздняк, И. С. Макаров. — Самара : ПГУТИ, 2020. — 43 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223313

2. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. — Йошкар-Ола : ПГТУ, 2020. — 154 с. — ISBN 978-5-8158-2165-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157473

Перечень дополнительной литературы

1. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – 3-е изд. – Москва : РИОР : ИНФРА-М, 2021. –400 с. – (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. Документ подписан простой электронной подписью Информация о владельце: ФИО: Петренко Вячеслав Иванович Должность: и.о. директора Института цифрового развития Дата подписания: 27.03.2024 16:03:15 Уникальный программный ключ: b47f96eea65a16e179f94dbf7fb0b10000e7ad4d

2. Астахов, А.М. Искусство управления информационными рисками [Электронный ресурс] / А.М. Астахов. – М. : ДМК Пресс, 2010. – 312 с. - ISBN 978-5-94074-574-7. - URL: http://biblioclub.ru/index.php? page=book&id=86481

3. Анисимов, А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. – М. : Интернет-Университет Информационных Технологий, 2009. - 176 с. - ISBN 9778-5-9963-0237-6. - URL: http://biblioclub.ru/index.php?page=book&id=232981

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ

УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

для обучающихся по организации и проведению самостоятельной работы

по дисциплине «Менеджмент инцидентов информационной безопасности информационных систем»

для студентов направления подготовки

_____

направленность (профиль):

_____

Ставрополь

2026

1. Общие положения

Самостоятельная работа – планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов). Владиславу Вячеславовичу

Самостоятельная работа студентов (СРС) в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.

К основным видам самостоятельной работы студентов относятся:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);

- написание докладов;

- подготовка к семинарам, практическим и лабораторным работам, их оформление;

- составление аннотированного списка статей из соответствующих журналов по отраслям знаний (педагогических, психологических, методических и др.);

- выполнение учебно-исследовательских работ, проектная деятельность;

- подготовка практических разработок и рекомендаций по решению проблемной ситуации;

- выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и т.д.;

- компьютерный текущий самоконтроль и контроль успеваемости на базе электронных обучающих и аттестующих тестов;

- выполнение курсовых работ (проектов) в рамках дисциплин;

- выполнение выпускной квалификационной работы и др.

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных качеств студентов и условий учебной деятельности.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

· подготовительный (определение целей, составление программы, подготовка методического обеспечения, подготовка оборудования);

· основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);

· заключительный (оценка значимости и анализ результатов, их систематизация, оценка эффективности программы и приемов работы, выводы о направлениях оптимизации труда).

Самостоятельная работа по дисциплине «Информационные технологии командной работы и проектной деятельности» направлена на формирование следующих **компетенций**:

Код	Формулировка
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

2. Цель и задачи самостоятельной работы

Ведущая цель организации и осуществления СРС совпадает с целью обучения студента – формирование набора общенаучных, профессиональных и универсальных компетенций будущего бакалавра.

При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности. Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

· систематизация и закрепление полученных теоретических знаний и практических умений студентов;

· углубление и расширение теоретических знаний;

· формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;

· развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;

· формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

· развитие исследовательских умений;

· использование материала, собранного и полученного в ходе самостоятельной работы и лабораторных занятий.

3. Технологическая карта самостоятельной работы студента

Коды реализуемых компете	Вид деятельности студентов	Итоговый продукт самостоя	Средства и технологии	Объем часов, в том числе (астр.)

нций		-тельной работы	оценки	СРС	Контактная работа с преподавателем	Всего
4 семестр						
УК-2	Подготовка к лекциям	Конспект лекций	Собеседование	14,25	15,0	29,25
УК-2	Подготовка к практическим занятиям	Отчет в электронном виде	Собеседование	14,25	15,0	29,25
УК-2	Самостоятельное изучение литературы	Конспект	Собеседование	14,25	15,0	29,25
УК-2	Самотестирование, подготовка к тестированию	Тестирование	Тестовые задания	14,25	15,0	29,25
Итого за 4 семестр				57,0	60,0	117,0
Итого				57,0	60,0	117,0

4. Контрольные точки и виды отчетности по ним

Контроль качества и сроков самостоятельной работы выполняется в соответствии с учебным графиком и оформляется в соответствии с заданием. Предусмотрена следующая рейтинговая оценка знаний

Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации.

Текущий контроль

5. Порядок выполнения самостоятельной работы студентом

5.1. Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют ***четыре основные установки в чтении научного текста***:

информационно-поисковый (задача – найти, выделить искомую информацию)

усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения излагаемые автором, так и всю логику его рассуждений)

аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

5.2. Методические рекомендации по составлению конспекта лекций:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта.
2. Выделите главное, составьте план.
3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора.
4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.
5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и

выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

5.3. Методические рекомендации по подготовке к практическим занятиям

Для того чтобы практические занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на лабораторных занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

Практические работы № 1-5,8 выполняются студентами заочной и очно-заочной формы обучения самостоятельно.

5.4. Методические рекомендации по самопроверке знаний

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется провести самопроверку усвоенных знаний, ответив на контрольные вопросы по изученной теме.

В случае необходимости нужно еще раз внимательно разобраться в материале.

Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала – умение отвечать на вопросы для собеседования.

Критерии оценки:

Оценка «отлично» выставляется студенту, если он, отлично знает, как моделировать технологические процессы создания и обработки материалов с учетом экономических факторов и требований экологической и промышленной безопасности. Уверенно владеет методами проектной деятельности, анализирует и оптимизирует технологические процессы, грамотно применяет инструменты, отлично знает, как внедрять новый проект в производство и управлять им на всех этапах его жизненного цикла. Уверенно владеет методами проектного управления, эффективно организует работу команды, оптимизирует ресурсы и контролирует реализацию проекта с учетом всех ключевых факторов.

Оценка «хорошо» выставляется студенту, если он, знает, как моделировать технологические процессы создания и обработки материалов с учетом экономических факторов и требований экологической и промышленной безопасности. Умеет анализировать технологические процессы, применять методы моделирования и учитывать ключевые экономические и экологические параметры, но может допускать отдельные неточности, знает, как внедрять новый проект в производство и управлять им на всех этапах его жизненного цикла. Умеет разрабатывать план реализации, организовывать работу команды и контролировать выполнение задач, но может допускать отдельные неточности в управлении ресурсами и сроками.

Оценка «удовлетворительно» выставляется студенту, если он, плохо знает, как моделировать технологические процессы создания и обработки материалов с учетом экономических факторов и требований экологической и промышленной безопасности. Испытывает трудности при анализе процессов, выборе подходящих методов и инструментов моделирования, допускает ошибки при учете экономических и экологических аспектов, плохо знает, как внедрять новый проект в производство и управлять им на всех этапах его жизненного цикла. Испытывает затруднения при планировании, организации и координации работ, допускает ошибки в управлении ресурсами и контроле выполнения задач.

Оценка «неудовлетворительно» выставляется студенту, если он, не знает, как моделировать технологические процессы создания и обработки материалов с учетом экономических факторов и требований экологической и промышленной безопасности. Не понимает принципов проектной деятельности и не способен применять соответствующие инструменты моделирования, не знает, как внедрять новый проект в производство и управлять им на всех этапах его жизненного цикла. Не понимает принципов проектного управления, не способен разрабатывать план реализации и контролировать выполнение задач

Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным 55. Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80

Удовлетворительный	60
Неудовлетворительный	0

5.6. Методические рекомендации по подготовке к зачетам

Контроль самостоятельной работы студентов

Контроль самостоятельной работы проводится преподавателем в аудитории.

Предусмотрены следующие виды контроля: собеседование, оценка выполнения доклада и его презентации.

Подробные критерии оценивания компетенций приведены в Фонде оценочных средств для проведения текущей и промежуточной аттестации.

6. Список литературы для выполнения СРС

Перечень основной литературы

1) Поздняк, И. С. Управление информационной безопасностью : методические указания / И. С. Поздняк, И. С. Макаров. — Самара : ПГУТИ, 2020. — 43 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223313
2) Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. — Йошкар-Ола : ПГТУ, 2020. — 154 с. — ISBN 978-5-8158-2165-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157473

Перечень дополнительной литературы

1) Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – 3-е изд. – Москва : РИОР : ИНФРА-М, 2021. –400 с. – (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. Документ подписан простой электронной подписью

Информация о владельце: ФИО: Петренко Вячеслав Иванович Должность: и.о. директора Института цифрового развития Дата подписания: 27.03.2024 16:03:15 Уникальный программный ключ: b47f96eea65a16e179f94dbf7fb0b10000e7ad4d

2) Астахов, А.М. Искусство управления информационными рисками [Электронный ресурс] / А.М. Астахов. – М. : ДМК Пресс, 2010. – 312 с. - ISBN 978-5-94074-574-7. - URL: http://biblioclub.ru/index.php? page=book&id=86481

3) Анисимов, А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. – М. : Интернет-Университет Информационных Технологий, 2009. - 176 с. - ISBN 9778-5-9963-0237-6. - URL: http://biblioclub.ru/index.php?page=book&id=232981

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Менеджмент инцидентов информационной безопасности информационных систем». Ставрополь : СКФУ, 2025.

2. Методические указания к практическим занятиям по дисциплине «Менеджмент инцидентов информационной безопасности информационных систем». Ставрополь : СКФУ, 2025.

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