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
«16» 05 2024 г.

Информационно-аналитические системы безопасности

Методические указания для самостоятельной работы по дисциплине «Информационно-аналитические системы безопасности» для студентов направления подготовки 10.04.01 «Информационная безопасность»

Курск 2024

УДК 004

Составители: Таныгин М.О., Кулешова Е.А.

Рецензент

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

Информационно-аналитические системы безопасности: методические указания для самостоятельной работы / Юго-Зап. гос. ун-т; сост.: М.О. Таныгин, Е.А. Кулешова. – Курск, 2024. – 13 с.: Библиогр.: с. 13.

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 16.05.24 . Формат 60x84 1/16.
Усл. печ.л. 0,7 Уч. –изд.л. 0,6 .Тираж 50 экз. Заказ 412
Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Содержание самостоятельной работы

	Тема СРС	Задание
1	Сущность, структура и задачи аналитики СБ.	**Описание задания:** Исследуйте и опишите основные принципы, структуру и задачи аналитики в области информационной безопасности. Обратите внимание на роль аналитики в обработке, интерпретации и использовании данных для обеспечения безопасности информации. **Требования:** • Напишите эссе или статью, в которой представлен анализ сущности и задач аналитики в области информационной безопасности. • Укажите конкретные примеры задач, которые решает аналитик в области безопасности данных. • Опишите влияние работы аналитика на принятие стратегических решений в сфере информационной безопасности.
2	Аналитика как интерфейс между теорией и практикой	**Описание задания:** Исследуйте роль аналитики как связующего элемента между теоретическими понятиями и практическими решениями в области информационной безопасности. Рассмотрите, как аналитика помогает преобразовать теоретические концепции в реальные стратегии и тактики по защите информации. **Требования:** • Составьте презентацию или доклад, подчеркивающий выбранную роль аналитики в СБ. • Приведите примеры реальных ситуаций, когда аналитика эффективно применялась для связи теории и практики в области информационной безопасности. • Обсудите преимущества использования аналитики как интерфейса между теорией и практикой в контексте СБ.

3	Принципы организации аналитической деятельности в СБ.	**Описание задания:** Изучите основные принципы, лежащие в основе организации аналитической деятельности в области информационной безопасности. Выявите, какие принципы являются ключевыми для успешной работы аналитика в области информационной безопасности. **Требования:** • Напишите исследовательскую статью, в которой рассматриваются основные принципы организации аналитической деятельности в СБ. • Сравните принципы аналитики в области информационной безопасности с другими областями аналитики. • Предложите рекомендации по применению ключевых принципов аналитики для оптимизации работы в области информационной безопасности.
4	Технологический цикл информационно-аналитической работы.	**Описание задания:** Исследуйте основные технологии и методы аналитики, применяемые в области информационной безопасности. Рассмотрите какие инструменты и подходы используются аналитиками для обработки, анализа и интерпретации данных в целях обеспечения безопасности информации. **Требования:** • Подготовьте обзорный доклад или презентацию о современных технологиях и методах аналитики в области информационной безопасности. • Приведите конкретные примеры использования различных технологий или методов аналитики в практике безопасности данных. • Проанализируйте преимущества и недостатки различных подходов к аналитике в области информационной безопасности.
5	Аналитический режим потребления информации.	**Описание задания:** Изучите основные направления развития профессиональных навыков аналитика в области

		информационной безопасности. Определите какие компетенции и умения необходимо развивать, чтобы быть эффективным специалистом в области аналитики информационной безопасности. **Требования:** • Напишите план по развитию профессиональных навыков аналитика в области СБ, включающий ключевые компетенции. • Обсудите влияние развития профессиональных навыков на успех аналитика в работе с данными информационной безопасности. • Предложите методы и подходы для саморазвития в области аналитики информационной безопасности.
6	Синтез информационно-аналитических СБ.	**Описание задания:** Студентам предлагается подготовить кейс-стадию о том, как синтез информационно-аналитических методов может быть применен для решения конкретной проблемы в области информационной безопасности. Они должны описать процесс синтеза - объединение различных методов и источников данных для создания цельного решения, и проанализировать его влияние на результаты. **Требования:** • Выбрать конкретную задачу или проблему в области информационной безопасности, которую можно решить с помощью синтеза информационно-аналитических методов. • Описать этапы синтеза, включая сбор данных, их анализ, выявление паттернов и тенденций, и, наконец, создание информационно-аналитического решения. • Проанализировать результаты применения синтеза и выделить ключевые выводы о его эффективности в контексте информационной безопасности.

7	Информационно аналитические системы аутентификации	**Описание задания:** Исследовать особенности информационно-аналитических систем аутентификации и систем защиты от несанкционированного доступа. Сравнить различные подходы к реализации этих систем, определить их преимущества и недостатки, и оценить их эффективность в защите информации. **Требования:** • Определить ключевые особенности информационно-аналитических систем аутентификации и защиты от несанкционированного доступа. • Провести анализ различных подходов к реализации этих систем, включая биометрическую идентификацию, двухфакторную аутентификацию, многофакторную аутентификацию и др. • Выявить преимущества и недостатки каждого вида системы, оценить их эффективность в предотвращении несанкционированного доступа к данным.
8	Информационно аналитические системы защиты от несанкционированного доступа (НСД).	**Задание:** 1. **Исследование информационно-аналитических систем НСД:** ○ Ознакомьтесь с концепцией информационно-аналитических систем защиты от несанкционированного доступа, изучите основные характеристики и задачи данных систем. 2. **Анализ принципов работы систем НСД:** ○ Рассмотрите принципиальные подходы к организации защиты информации с использованием информационно-аналитических систем. Изучите, как эти системы обнаруживают и предотвращают несанкционированный доступ. 3. **Сравнительный анализ различных видов систем НСД:** ○ Сравните различные виды информационно-аналитических систем защиты от

		несанкционированного доступа, такие как системы мониторинга, системы идентификации и аутентификации, системы анализа поведения пользователей и т.д. 4. **Оценка преимуществ и недостатков различных подходов:** ○ Выделите основные преимущества и недостатки каждого вида информационно-аналитических систем защиты от несанкционированного доступа. Рассмотрите их эффективность, сложность внедрения и управления. 5. **Разработка рекомендаций по выбору и реализации систем НСД:** ○ На основе проведенного анализа выработайте рекомендации по выбору наиболее подходящего типа информационно-аналитической системы защиты от несанкционированного доступа для конкретной среды или организации. **Требования к заданию:** 1. Глубокое понимание информационно-аналитических систем защиты от несанкционированного доступа. 2. Объективный сравнительный анализ различных подходов и их практическое применение. 3. Способность к формированию аргументированных рекомендаций по выбору и внедрению систем НСД. 4. Подготовка доклада с обоснованием результатов и выводов.

КОНТРОЛЬНЫЕ ВОПРОСЫ

Тема 1. Сущность, структура и задачи аналитики СБ.

1. Что представляет собой сущность аналитики в области безопасности (СБ)?
2. Каковы основные задачи аналитики СБ при обеспечении безопасности организации?
3. Какие компоненты входят в структуру аналитической работы в области СБ?
4. Каким образом аналитика СБ способствует выявлению и анализу угроз безопасности?
5. Как важна аналитика СБ для принятия эффективных решений и разработки стратегии безопасности организации?
6. Какие методы и техники используются аналитиками СБ для предотвращения инцидентов безопасности?
7. Каким образом аналитика СБ помогает в поиске и раскрытии внутренних угроз?
8. Как аналитическая работа в области СБ помогает в предсказании и прогнозировании возможных угроз безопасности?
9. Как влияет аналитика СБ на эффективность и результативность действий оперативных служб по обеспечению безопасности?
10. Какие навыки и компетенции требуются у аналитиков СБ для успешного выполнения своих задач?

Тема 2. Аналитика как интерфейс между теорией и практикой.

1. Как аналитика в области СБ выполняет роль интерфейса между теорией и практикой?
2. Как аналитика СБ помогает в переводе теоретических сведений в конкретные действия и решения?
3. Какие методы и инструменты используются аналитиками СБ для преобразования теории в практические рекомендации?
4. Как аналитика СБ связывает технические аспекты безопасности с бизнес-потребностями организации?
5. Как аналитика СБ помогает в оценке эффективности существующих политик и процедур безопасности и вносит рекомендации по их улучшению?
6. Каким образом аналитика СБ учитывает динамику развития технологий и угроз в своей работе?
7. Как аналитика СБ помогает в обучении и развитии персонала, осознавать значимость безопасности и соблюдать соответствующие процедуры?
8. Какие вызовы и проблемы возникают при переводе теории в практику через аналитический процесс СБ?

9. Как аналитика СБ содействует передаче знаний и опыта между различными уровнями и подразделениями организации?

10. Каким образом аналитика СБ способствует повышению информированности и осведомленности руководства о текущей ситуации с безопасностью?

Тема 3. Принципы организации аналитической деятельности в СБ.

1. Какие принципы лежат в основе организации аналитической деятельности в области СБ?

2. Как принцип коллективности влияет на эффективность аналитической работы в СБ?

3. Как принцип системности помогает обеспечить полноту и объективность аналитических исследований в СБ?

4. Как принцип актуальности обеспечивает своевременное выявление и реагирование на угрозы безопасности?

5. Как принцип конфиденциальности влияет на сохранение и защиту информации в аналитической деятельности СБ?

6. Как принцип независимости гарантирует объективность и непредвзятость аналитических выводов в СБ?

7. Как принцип постоянного обучения и развития способствует повышению профессионального уровня аналитиков СБ?

8. Каким образом принцип сегментации информации влияет на эффективность аналитической работы в СБ?

9. Как принцип оперативности и своевременности способствует эффективному реагированию на изменения среды и угроз безопасности?

10. Как принцип прозрачности и документирования помогает обеспечить юридическую значимость и анализируемости аналитической работы в СБ?

Тема 4. Технологический цикл информационно-аналитической работы.

1. Каковы этапы технологического цикла информационно-аналитической работы в области СБ?

2. Что включает первый этап технологического цикла - сбор информации в аналитике СБ?

3. Как осуществляется анализ и интерпретация собранных данных в информационно-аналитической работе СБ?

4. Каким образом принимаются решения и формулируются рекомендации на основе проведенного анализа в технологическом цикле СБ?

5. Каким способом осуществляется контроль и обратная связь на завершающем этапе технологического цикла информационно-аналитической работы в СБ?

6. Какие методы и инструменты используются на этапе сбора информации в аналитике СБ?

7. Как аналитика СБ выбирает и применяет методы структурирования и анализа данных на этапе обработки информации?

8. Как представление информации и ее визуализация влияют на эффективность аналитического процесса в СБ?

9. Какие подходы используются для автоматизации и оптимизации технологического цикла информационно-аналитической работы в аналитике СБ?

10. Как информационно-аналитическая работа в СБ учитывает требования по защите данных и конфиденциальности?

Тема 5. Аналитический режим потребления информации.

1. Что представляет собой аналитический режим потребления информации в области СБ?

2. Какой подход следует использовать для построения аналитического режима потребления информации в аналитике СБ?

3. Как аналитический режим помогает в обнаружении скрытых угроз и аномалий в информационной безопасности?

4. Каким образом аналитический режим способствует эффективному использованию информации для принятия решений в СБ?

5. Какие преимущества получает организация при внедрении аналитического режима потребления информации в аналитике СБ?

6. Какие навыки и инструменты необходимы аналитику СБ для эффективного использования аналитического режима?

7. Как аналитический режим помогает в прогнозировании и предотвращении инцидентов безопасности?

8. Как аналитический режим способствует постоянному мониторингу и анализу потенциальных угроз безопасности?

9. Каким образом аналитический режим фокусируется на поиске новых трендов и возможных уязвимостей?

10. Как аналитический режим потребления информации способствует принятию оперативных мер и реагированию на угрозы безопасности в реальном времени?

Тема 6. Синтез информационно-аналитических СБ.

1. Что означает синтез информационно-аналитических решений в области СБ?

2. Какие методы и подходы применяются для синтеза информационно-аналитических СБ?

3. Как синтез информационно-аналитических решений помогает преодолеть сложности и неопределенность в области безопасности?

4. Каким образом синтез информационно-аналитических СБ способствует выявлению скрытых связей и паттернов в данных?

5. Как аналитика СБ интегрирует различные источники информации и аналитические методы для синтеза полной картины безопасности?

6. Как синтез информационно-аналитических решений помогает прогнозированию и предотвращению будущих угроз безопасности?
7. Как аналитика СБ применяет синтез информационно-аналитических решений для разработки стратегии безопасности организации?
8. Какие вызовы и проблемы возникают при синтезе информационно-аналитических решений в области СБ?
9. Каким образом синтез информационно-аналитических СБ помогает в принятии комплексных и обоснованных решений в области безопасности?
10. Как аналитика СБ управляет информацией, полученной в результате синтеза, для предоставления ценных выводов и рекомендаций?

Тема 7. Информационно аналитические системы аутентификации.

1. Что представляют собой информационно-аналитические системы аутентификации?
2. Как работают информационно-аналитические системы аутентификации для обеспечения безопасности?
3. Какие основные методы и технологии используются в информационно-аналитических системах аутентификации?
4. Как информационно-аналитические системы аутентификации обеспечивают защиту от подделки или манипуляции идентификационных данных?
5. Каким образом информационно-аналитические системы аутентификации способствуют контролю и управлению доступом к информации?
6. Как информационно-аналитические системы аутентификации используют анализ поведения пользователей для определения аномалий и потенциальных угроз?
7. Каким образом информационно-аналитические системы аутентификации применяют многофакторную аутентификацию для повышения безопасности?
8. Как информационно-аналитические системы аутентификации обеспечивают учет и аудит доступа к информации?
9. Какие вызовы и проблемы возникают при разработке и использовании информационно-аналитических систем аутентификации?
10. Как информационно-аналитические системы аутентификации способствуют удовлетворению требований по безопасности данных и соответствию нормативным актам в области безопасности?

Тема 8. Информационно аналитические системы защиты от несанкционированного доступа (НСД).

1. Как работают информационно-аналитические системы НСД для обеспечения безопасности?

2. Какие методы и технологии используются в информационно-аналитических системах НСД для обнаружения и предотвращения атак?
3. Как информационно-аналитические системы НСД помогают в обнаружении уязвимостей и слабых мест в защите информации?
4. Как информационно-аналитические системы НСД реагируют на аномальное поведение и атаки в реальном времени?
5. Каким образом информационно-аналитические системы НСД анализируют события и логи для выявления инцидентов безопасности?
6. Как информационно-аналитические системы НСД используют искусственный интеллект и машинное обучение?
7. Какие информационно аналитические системы защиты от несанкционированного доступа (НСД)?
8. Какие преступления в области НСД в России Вам известны?
9. Что представляют собой информационно-аналитические системы защиты от несанкционированного доступа (НСД)?
10. Что такое НСД? Виды НСД.

ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННЫХ РЕСУРСОВ

1. Ипатова, Э. Р. Методологии и технологии системного проектирования информационных систем : учебник / Э. Р. Ипатова, Ю. В. Ипатов. – 3-е изд., стер. – Москва : ФЛИНТА, 2021. – 256 с. – URL: https://biblioclub.ru/index.php?page=book&id=79551 (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.

2. 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: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.

3. Аверченков, В. И. История развития системы государственной безопасности России : учебное пособие / В. И. Аверченков, В. В. Ерохин, О. М. Голембиовская ; науч. ред. Ю. Т. Трифанков. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 193 с. – URL: https://biblioclub.ru/index.php?page=book&id=93267 (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.

4. Алдохина, О. И. Информационно-аналитические системы и сети : учебное пособие / О. И. Алдохина, О. Г. Басалаева. – Кемерово : КемГУКИ, 2010. – Часть 1. Информационно-аналитические системы. – 148 с. – URL: https://biblioclub.ru/index.php?page=book&id=227684 (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.

5. 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: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.