

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Локтионова Оксана Геннадьевна  
Должность: проректор по учебной работе  
Дата подписания: 18.09.2023 16:59:22  
Уникальный программный ключ:  
0b817ca911e6668abb13a5d48e39170e4851104561089

## МИНОБРНАУКИ РОССИИ

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

Кафедра информационной безопасности

УТВЕРЖДАЮ

Проректор по учебной работе

О.Г. Локтионова

« 8 » 08

2023 г.



### Управление разработкой систем безопасности

Методические указания по организации самостоятельной  
работы по дисциплине «Управление разработкой систем  
безопасности» для студентов направления подготовки  
10.04.01 «Информационная безопасность»

УДК 004.773.5

Составители: Кулешова Е.А.

Рецензент

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

**Управление разработкой систем безопасности:**  
методические указания для самостоятельной работы / Юго-Зап. гос.  
ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 8 с.: Библиогр.: с. 8.

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	Основные аспекты построения системы информационной безопасности.	<ol style="list-style-type: none"> <li>1. Изучите ключевые компоненты и принципы, необходимые при построении системы информационной безопасности (СИБ).</li> <li>2. Разработайте план построения СИБ для конкретной организации, включающий оценку рисков, разработку политик и процедур, внедрение технических средств безопасности и обучение персонала.</li> <li>3. Проанализируйте примеры успешной реализации СИБ и определите основные факторы успеха и препятствия при ее внедрении.</li> </ol>
2	Мероприятия по защите информации.	<ol style="list-style-type: none"> <li>1. Исследуйте различные мероприятия по защите информации, такие как аутентификация, авторизация, шифрование данных, контроль доступа и мониторинг.</li> <li>2. Разработайте план мероприятий по защите информации для организации, включающий выбор и внедрение соответствующих технических и организационных средств безопасности.</li> <li>3. Проанализируйте примеры использования мероприятий по защите информации в сфере бизнеса и оцените их эффективность.</li> </ol>
3	Требования к архитектуре ИС для обеспечения безопасности ее функционирования.	<ol style="list-style-type: none"> <li>1. Изучите основные требования к архитектуре информационной системы (ИС), которые обеспечивают ее безопасное функционирование.</li> <li>2. Разработайте модель архитектуры ИС для конкретной организации, учитывая требования к безопасности, такие как разделение прав доступа, контроль интеграции систем и обеспечение конфиденциальности данных.</li> <li>3. Проанализируйте примеры применения требований к архитектуре ИС в реальных организациях и оцените их эффективность.</li> </ol>
4	Оценочные стандарты и технические спецификации	<ol style="list-style-type: none"> <li>1. Исследуйте различные оценочные стандарты и технические спецификации, используемые для оценки безопасности информационных технологий (ИТ).</li> <li>2. Сравните и проанализируйте характеристики и</li> </ol>

		<p>требования различных стандартов и спецификаций, таких как ISO / IEC 27001, NIST SP 800-53, Common Criteria и другие.</p> <p>3. Определите, какой стандарт или спецификация наиболее удобна для оценки безопасности ИТ в конкретной ситуации.</p>
5	Критерии оценки безопасности информационных технологий.	<p>1. Изучите различные критерии оценки безопасности информационных технологий, такие как конфиденциальность, целостность, доступность и непрерывность.</p> <p>2. Разработайте методику оценки безопасности ИТ, включающую определение соответствующих критериев, выбор адекватных метрик и оценку степени защищенности системы.</p> <p>3. Проанализируйте примеры оценки безопасности ИТ на основе выбранных критериев и оцените их эффективность.</p>
6	Руководящие документы ФСТЭК России.	<p>1. Исследуйте руководящие документы ФСТЭК России, связанные с обеспечением информационной безопасности в Российской Федерации.</p> <p>2. Разберитесь, какие требования и рекомендации предлагает ФСТЭК России по различным аспектам информационной безопасности, таким как защита персональных данных, средства защиты информации и управление информационной безопасностью.</p> <p>3. Проанализируйте влияние руководящих документов ФСТЭК России на практику обеспечения информационной безопасности в России.</p>

## КОНТРОЛЬНЫЕ ВОПРОСЫ

### **Тема 1. Основные аспекты построения системы информационной безопасности.**

1. Перечислите основные методы и средства защиты информации.
2. Дайте определения кодирования и декодирования.
3. Как осуществляется защита от несанкционированного доступа к данным?
4. Охарактеризуйте классы безопасности компьютерных систем.
5. Сформулируйте определение электронной цифровой подписи.
6. Какие ресурсы системы должны быть защищаемы и в какой степени?
7. Какова должна быть полная стоимость реализации защиты и затраты на эксплуатацию с учетом потенциальных угроз?
8. Какие угрозы должны быть устранены и в какой мере?
9. Что предполагает статическая целостность информации?
10. С помощью каких средств должна быть реализована защита?

### **Тема 2. Мероприятия по защите информации.**

1. Какие механизмы обеспечения безопасности существуют?
2. Перечислите основные технологические мероприятия комплексной системы обеспечения информационной безопасности.
3. Какие проблемы информационной безопасности вы знаете?
4. Составляющие информационной безопасности.
5. Система формирования информационной безопасности.
6. Какие существуют модели защиты информации?
7. Что предполагает динамическая целостность информации?
8. Понятие конфиденциальности в информационной безопасности.
9. Перечислите основные мероприятия организации работ по обеспечению защиты информации.
10. Какие существуют уровни формирования информационной безопасности?

### **Тема 3. Требования к архитектуре ТКС для обеспечения безопасности ее функционирования.**

1. Правильно построенная архитектура решает некоторые проблемы ИБ сетей?
2. Перечислите требования, предъявляемые к системам защиты информации.
3. Перечислите основные методы и средства обеспечения защиты информации.

4. Что включают в себя организационные средства обеспечения защиты информации?
5. Характеристика системы обнаружения вторжений (СОВ).
6. Основные методы защиты от атак на сетевую инфраструктуру.
7. Характеристика технических мер защиты от сетевых атак.
8. Что включают в себя программно-аппаратные средства защиты информации?
9. Руководящий документ «Классификация автоматизированных систем.
10. Что включают в себя инженерно-технические средства защиты информации?

#### **Тема 4. Оценочные стандарты и технические спецификации.**

1. Комплекс документов Банка России СТО БР ИББС, краткая характеристика, показатели ИБ. Способы оценивания показателей.
2. Понятие «стандарт», краткая характеристика «Оранжевой книги».
3. Что понимается под термином «политика безопасности»?
4. Характеристика стандарта ГОСТ Р ИСО/МЭК 15408
5. Что понимается под термином «уровень гарантированности»?
6. Перечислите методы и стандарты шифрования.
7. Опишите стандарты безопасности (WPA, WPA2). VPN.
8. Что понимается под термином «операционная гарантированность»?
9. Международные стандарты менеджмента ИБ серии ISO 27000. Модель PDCA, стандарты NIST.
10. Какие классы стандартов безопасности вы знаете?

#### **Тема 5. Критерии оценки безопасности информационных технологий.**

1. Опишите иерархию сущностей в "Критериях оценки безопасности информационных технологий".
2. Назовите основные термины, описанные в "Критериях оценки безопасности информационных технологий".
3. Опишите структуру класса «приватность».
4. Опишите структуру класса «использование ресурсов».
5. Что такое требования доверия безопасности и для чего они нужны?
6. Что такое уровни доверия?
7. Какие существуют механизмы обеспечения безопасности в распределённых системах?
8. Какие 3 составляющих информационной безопасности вы знаете?

9. Что является критерием безопасности?
10. Какие основные критерии и методологии используются для оценки безопасности информационных технологий?

### **Тема 6. Руководящие документы ФСТЭК России.**

1. Какие руководящие документы ФСТЭК России существуют?  
Понятие "государственная тайна".
2. Что контролирует ФСТЭК?
3. Руководящий документ «Классификация по уровню контроля отсутствия недеklarированных возможностей», характеристика, основные моменты.
4. Что такое сертификат ФСТЭК?
5. Кто руководит ФСТЭК?
6. Кто регулирует деятельность в области защиты информации?
7. Чем отличается ФСТЭК от фсб?
8. Кто выдает лицензию ФСТЭК?
9. Кому подчиняется ФСТЭК России?
10. Руководящий документ «СВТ. Показатели защищенности от НСД к информации», характеристика, основные моменты.

**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. Марухленко, А. Л. Разработка защищённых интерфейсов Web-приложений : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов. – Москва ; Берлин : Директ-Медиа, 2021. – 175 с. – URL: <https://biblioclub.ru/index.php?page=book&id=599050> (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.
3. Абрамов, Г. В. Проектирование информационных систем : учебное пособие / Г. В. Абрамов, И. Е. Медведкова, Л. А. Коробова. – Воронеж : Воронежский государственный университет инженерных технологий, 2012. – 172 с. – URL: <https://biblioclub.ru/index.php?page=book&id=141626> (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.
4. Петренко, В. И. Теоретические основы защиты информации : учебное пособие / В. И. Петренко ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2015. – 222 с. – URL: <https://biblioclub.ru/index.php?page=book&id=458204> (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.
5. Аверченков, В. И. Служба защиты информации : организация и управление : учебное пособие / В. И. Аверченков, М. Ю. Рытов. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 186 с. – URL: <https://biblioclub.ru/index.php?page=book&id=93356> (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.