

Министерство науки и высшего образования Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Владимирский государственный университет  
имени Александра Григорьевича и Николая Григорьевича Столетовых»  
(ВлГУ)

Институт информационных технологий и радиоэлектроники

(Наименование института)

УТВЕРЖДАЮ:

Директор института

  
А.А. Галкин

« 26 » августа 2021 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**  
**ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ**

(наименование дисциплины)

**направление подготовки / специальность**

**10.05.04 «Информационно-аналитические системы безопасности»**

(код и наименование направления подготовки (специальности))

**направленность (профиль) подготовки**

**Автоматизация информационно-аналитической деятельности**

(направленность (профиль) подготовки))

г. Владимир

2021 год

## 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Основы управления информационной безопасностью» являются обеспечение подготовки студентов в соответствии с требованиями ФГОС ВО 3++ и учебного плана по специальности 10.05.04 «Информационно-аналитические системы безопасности». В процессе подготовки обеспечивается формирование у студентов обобщенного представления об основных принципах и возможностях обеспечения управления информационной безопасностью на объекте защиты.

В ходе освоения дисциплины проводится ознакомление студентов с механизмами создания системы управления информационной безопасностью, контроля за работой средств управления (СУИБ) на предприятии. Рассматривается мониторинг и оценка рисков управления информационной безопасностью.

Задачей дисциплины «Основы управления информационной безопасностью» является освоение принципов реализации и основных подходов к оптимальному управлению различными механизмами информационной безопасности в автоматизированных информационных системах (АИС). В процессе освоения дисциплины изучаются следующие вопросы: основные руководящие документы и показатели эффективности системы защиты информации; комплексный подход к обеспечению ИБ; цели, стратегии и политика информационной безопасности; организационные аспекты информационной безопасности; функции управления информационной безопасностью; процессный подход для управления информационной безопасностью; система ответственности в области информационной безопасности; организация и методика проведения аудита системы управления информационной безопасностью; алгоритм проведения анализа информационных рисков в КИС предприятия; аналитические технологии управления ИБ; обеспечение управления ИБ в чрезвычайных ситуациях. Задачей дисциплины также является овладение навыками практической деятельности в области моделирования и анализа технических средств управления информационной безопасностью в АИС с использованием средств вычислительной техники, умение использовать соответствующее специализированное программное обеспечение.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Основы управления информационной безопасностью» относится к обязательной части Блока Б1 (код Б1.О.18). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций, лабораторных работ и самостоятельной работы студентов. Курс тесно взаимосвязан с другими дисциплинами данного цикла.

## 3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции	Результаты обучения по дисциплине	
<b>УК-2</b> Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1.1	Знать этапы жизненного цикла проекта, методы разработки и управления проектами	Тестовые вопросы
	УК-2.2.1	Уметь определять цели и задачи проекта; разрабатывать план реализации проекта, представлять промежуточные и итоговый отчеты по проекту	
	УК-2.3.1	Владеть навыками разработки проектов в избранной профессиональной сфере, методами оценки эффективности проекта	

<b>УК-3</b> Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.1.1	Знать методы эффективного руководства коллективом, способы и приемы установления взаимоотношений и коммуникации в рамках командного взаимодействия	Тестовые вопросы
	УК-3.1.2	Знать основные механизмы информационной безопасности и типовые процессы управления этими механизмами в автоматизированной системе	
	УК-3.1.3	Знать основные угрозы безопасности информации и модели нарушителя в информационных системах	
	УК-3.1.4	Знать принципы формирования политики информационной безопасности в информационных системах	
	УК-3.1.5	Знать основы теории рисков информационной безопасности	
	УК-3.1.6	Знать основные модели, стандарты и нормативно-распорядительные документы государственных регуляторов по вопросам управления процессами обеспечения информационной безопасности	
	УК-3.2.1	Уметь эффективно взаимодействовать с членами команды, соблюдая нормативно-правовые и этические нормы, планировать работу команды	
	УК-3.2.2	Уметь создавать формальные модели управления процессами обеспечения информационной безопасности	
	УК-3.2.3	Уметь прогнозировать состояние информационной безопасности объекта защиты на основе использования теории рисков	
	УК-3.3.1	Владеть навыками организации и руководства команды при реализации совместно выработанной командной стратегии достижения поставленной цели	
	УК-3.3.2	Владеть основными системными подходами к определению целей, задач обеспечения информационной безопасности в автоматизированных системах	
	УК-3.3.3	Владеть основными навыками поиска информации о современных и перспективных методах обеспечения информационной безопасности в автоматизированных системах и поиска источников специальной информации, необходимой в профессиональной деятельности	
<b>УК-9</b> Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-9.1.1	Знать основные законы и закономерности функционирования экономики, основы экономической теории, необходимые для решения профессиональных и социальных задач	Тестовые вопросы
	УК-9.2.1	Уметь оценивать степень риска продуктов и услуг финансовых институтов и на основании этого принимать обоснованные экономические решения	
	УК-9.3.1	Владеть навыками грамотно определять финансовые цели в различных областях жизнедеятельности на основе сбора и анализа финансовой информации	

#### 4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 3 зачетных единицы, 108 часов

**Тематический план  
форма обучения – очная**

№ п/п	Наименование тем и/или разделов/тем дисциплины	Семестр	Неделя семестра	Контактная работа обучающихся с педагогическим работником				Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации (по семестрам)
				Лекции	Практические занятия	Лабораторные работы	в форме практической работы		
1	<b>Раздел 1.</b> Основные понятия и подходы к управлению информационной безопасностью.	6	1	2				2	
2	<b>Раздел 2.</b> Система управления информационной безопасностью. Политика информационной безопасности.	6	2	2		4		2	
3	<b>Раздел 3.</b> Процессный подход для управления информационной безопасностью.	6	3	2				2	
4	<b>Раздел 4.</b> Основные критерии выбора средств управления информационной безопасностью на предприятии.	6	4	2		4		2	
5	<b>Раздел 5.</b> Основные виды угроз информационной безопасности.	6	5	2				2	
6	<b>Раздел 6.</b> Мероприятия по управлению информационной безопасностью на предприятии.	6	6	2		4		2	Рейтинг-контроль №1
7	<b>Раздел 7.</b> Контроль за работой средствами управления информационной безопасности (СУИБ) на предприятии.	6	7	2				2	
8	<b>Раздел 8.</b> Политика информационной безопасности.	6	8	2		4		2	
9	<b>Раздел 9.</b> Угрозы информационной безопасности. Построение модели угроз.	6	9	2				2	
10	<b>Раздел 10.</b> Причинно-следственный анализ угроз и уязвимостей в системе управления информационной безопасностью предприятия.	6	10	2		4		2	
11	<b>Раздел 11.</b> Анализ и оценка рисков информационной безопасности предприятия.	6	11	2				2	
12	<b>Раздел 12.</b> Положение о применимости результатов в СУИБ.	6	12	2		4		2	Рейтинг-контроль №2

13	<b>Раздел 13.</b> Контроль защищенности автоматизированных систем.	6	13	2			2	
14	<b>Раздел 14.</b> Требования по обеспечению защиты информации в АИС, классификация АИС.	6	14	2		4	2	
15	<b>Раздел 15.</b> Инвентаризация информационных актив в АИС.	6	15	2			2	
16	<b>Раздел 16.</b> Уязвимости в АИС и способы их выявления.	6	16	2		4	2	
17	<b>Раздел 17.</b> Требования нормативно-правовых документов и стандартов в области управления ИБ.	6	17	2			2	
18	<b>Раздел 18.</b> Обеспечение ИБ в чрезвычайных ситуациях.	6	18	2		4	2	Рейтинг-контроль №3
Итого по дисциплине		<b>108</b>		<b>36</b>		<b>36</b>	<b>36</b>	<b>Зачет</b>

### Содержание лекционных занятий по дисциплине

**Раздел 1.** Основные понятия и подходы к управлению информационной безопасностью. Составляющие информационной безопасности на предприятии. Нормативно-правовые аспекты и методы регулирования в области информационной безопасности.

**Раздел 2.** Система управления информационной безопасностью. Политика информационной безопасности. Организационные аспекты информационной безопасности

**Раздел 3.** Процессный подход для управления информационной безопасностью. Система ответственности в области информационной безопасности

**Раздел 4.** Основные критерии выбора средств управления информационной безопасностью на предприятии. Перечень защищаемой информации на предприятии. Формирование матрицы и модели доступа к управлению информационной безопасностью.

**Раздел 5.** Основные виды угроз информационной безопасности. Модель нарушителя информационной безопасности.

**Раздел 6.** Мероприятия по управлению информационной безопасностью на предприятии. Определение режима управления информацией на предприятии. Разработка подсистемы управления доступом защищаемой информации.

**Раздел 7.** Контроль за работой средствами управления информационной безопасности (СУИБ) на предприятии. Мониторинг и оценка рисков управления информационной безопасностью.

**Раздел 8.** Политика информационной безопасности. Содержание Политики информационной безопасности. Порядок разработки Политики информационной безопасности.

**Раздел 9.** Угрозы информационной безопасности. Построение модели угроз. Классификация угроз. Типовая модель угроз информационной безопасности. Определение актуальных угроз информационной безопасности.

**Раздел 10.** Причинно-следственный анализ угроз и уязвимостей в системе управления информационной безопасностью предприятия. Документированные процедуры угроз ИБ.

**Раздел 11.** Анализ и оценка рисков информационной безопасности предприятия. Оценка информационных рисков на основе причинно-следственных связей угроз и уязвимостей. Алгоритм оценки информационных рисков организации на основе причинно-следственных связей угроз и уязвимостей.

**Раздел 12.** Положение о применимости результатов в СУИБ.

**Раздел 13.** Контроль защищенности автоматизированных систем. Задачи, возникающие в ходе контроля защищенности.

**Раздел 14.** Требования по обеспечению защиты информации в АИС, классификация АИС.

**Раздел 15.** Инвентаризация информационных актив в АИС. Объекты и способы инвентаризации. Инвентаризация с помощью сетевого сканера. Инвентаризация с использованием системных проверок.

**Раздел 16.** Уязвимости в АИС и способы их выявления. Понятие уязвимости и категории проверок. Тесты и эксплойты. Выявление уязвимостей по косвенным признакам.

**Раздел 17.** Требования нормативно-правовых документов и стандартов в области управления ИБ.

**Раздел 18.** Обеспечение ИБ в чрезвычайных ситуациях. План обеспечения управления ИБ предприятия в чрезвычайных ситуациях.

### **Содержание практических/лабораторных занятий по дисциплине**

**Лабораторная работа №1.** Формирование базы данных текущего состояния АИС на предприятии (по вариантам), в том числе и защищенности ИР в АИС.

**Лабораторная работа №2.** Формирование перечня защищаемой информации на предприятии (по вариантам). Формирование матрицы и модели доступа к управлению информационной безопасностью.

**Лабораторная работа №3.** Классификация АИС предприятия (по вариантам) по требованиям руководящего документа ФСТЭК России РД.1992.03.30.1 «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»

**Лабораторная работа №4.** Формирование модели нарушителя информационной безопасности в АИС на предприятии (по вариантам).

**Лабораторная работа №5.** Формирование политики ИБ в организации (по вариантам) с учетом частной модели угроз для АИС и модели нарушителя в АИС.

**Лабораторная работа №6.** Определение класса защищенности информационной системы согласно приказов ФСТЭК России №17-2013г. и №27-2017г. для ГИС, не содержащих сведений, составляющих государственную тайну.

**Лабораторная работа №7.** Определение состава базовых мер защиты информации для соответствующего класса защищенности ГИС (не содержащих сведений, составляющих государственную тайну), согласно приказов ФСТЭК России №17-2013г. и №27-2017г.

**Лабораторная работа №8.** Определение актуальности угроз для ИСПдН в АИС (по вариантам), согласно методике определения актуальных угроз безопасности, персональных данных при их обработке в информационных системах персональных данных ФСТЭК России

**Лабораторная работа №9.** Формирование Политики оператора АИС на предприятии (по вариантам) в отношении обработки персональных данных согласно рекомендациям ФСТЭК России

## **5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ**

### **5.1. Текущий контроль успеваемости**

#### **Перечень вопросов к рейтинг-контролю №1**

- Основные понятия и подходы к управлению информационной безопасностью.
- Составляющие информационной безопасности на предприятии.
- Нормативно-правовые аспекты и методы регулирования в области информационной безопасности.
- Система управления информационной безопасностью. Политика информационной безопасности.

- Организационные аспекты управления информационной безопасности
- Процессный подход для управления информационной безопасностью. Система ответственности в области информационной безопасности.
- Основные критерии выбора средств управления информационной безопасностью на предприятии.
- Перечень защищаемой информации на предприятии.
- Формирование матрицы и модели доступа к управлению информационной безопасностью.
- Основные виды угроз информационной безопасности.
- Модель нарушителя информационной безопасности.
- Мероприятия по управлению информационной безопасностью на предприятии.

### **Перечень вопросов к рейтинг-контролю №2**

- Определение режима управления информацией на предприятии.
- Разработка подсистемы управления доступом защищаемой информации.
- Контроль за работой средствами управления информационной безопасности (СУИБ) на предприятии.
- Мониторинг и оценка рисков управления информационной безопасностью.
- Политика информационной безопасности. Содержание Политики информационной безопасности.
- Порядок разработки Политики информационной безопасности.
- Угрозы информационной безопасности. Построение модели угроз.
- Классификация угроз. Типовая модель угроз информационной безопасности.
- Определение актуальных угроз информационной безопасности.
- Причинно-следственный анализ угроз и уязвимостей в системе управления информационной безопасностью предприятия.
- Документированные процедуры угроз ИБ.
- Анализ и оценка рисков информационной безопасности предприятия.

### **Перечень вопросов к рейтинг-контролю №3**

- Оценка информационных рисков на основе причинно-следственных связей угроз и уязвимостей.
- Алгоритм оценки информационных рисков организации на основе причинно-следственных связей угроз и уязвимостей.
- Положение о применимости результатов в СУИБ.
- Контроль защищенности автоматизированных систем. Задачи, возникающие в ходе контроля защищенности.
- Требования по обеспечению защиты информации в АИС, классификация АИС.
- Инвентаризация информационных актив в АИС. Объекты и способы инвентаризации. Инвентаризация информационных актив в АИС с помощью сетевого сканера.
- Инвентаризация информационных актив в АИС с использованием системных проверок.
- Уязвимости в АИС и способы их выявления. Понятие уязвимости и категории проверок.
- Выявление уязвимостей в АИС с использованием тестов и эксплойтов.
- Выявление уязвимостей в АИС по косвенным признакам.
- Основные требования нормативно-правовых документов и стандартов в области управления ИБ.
- Обеспечение ИБ в чрезвычайных ситуациях. План обеспечения управления ИБ предприятия в чрезвычайных ситуациях.

## 5.2. Промежуточная аттестация

### Примерный перечень вопросов к зачету

1. Основные понятия и подходы к управлению информационной безопасностью.
2. Составляющие информационной безопасности на предприятии.
3. Нормативно-правовые аспекты и методы регулирования в области информационной безопасности.
4. Система управления информационной безопасностью. Политика информационной безопасности.
5. Организационные аспекты управления информационной безопасности
6. Процессный подход для управления информационной безопасностью. Система ответственности в области информационной безопасности.
7. Основные критерии выбора средств управления информационной безопасностью на предприятии.
8. Перечень защищаемой информации на предприятии.
9. Формирование матрицы и модели доступа к управлению информационной безопасностью.
10. Основные виды угроз информационной безопасности.
11. Модель нарушителя информационной безопасности.
12. Мероприятия по управлению информационной безопасностью на предприятии.
13. Определение режима управления информацией на предприятии.
14. Разработка подсистемы управления доступом защищаемой информации.
15. Контроль за работой средствами управления информационной безопасности (СУИБ) на предприятии.
16. Мониторинг и оценка рисков управления информационной безопасностью.
17. Политика информационной безопасности. Содержание Политики информационной безопасности.
18. Порядок разработки Политики информационной безопасности.
19. Угрозы информационной безопасности. Построение модели угроз.
20. Классификация угроз. Типовая модель угроз информационной безопасности.
21. Определение актуальных угроз информационной безопасности.
22. Причинно-следственный анализ угроз и уязвимостей в системе управления информационной безопасностью предприятия.
23. Документированные процедуры угроз ИБ.
24. Анализ и оценка рисков информационной безопасности предприятия.
25. Оценка информационных рисков на основе причинно-следственных связей угроз и уязвимостей.
26. Алгоритм оценки информационных рисков организации на основе причинно-следственных связей угроз и уязвимостей.
27. Положение о применимости результатов в СУИБ.
28. Контроль защищенности автоматизированных систем. Задачи, возникающие в ходе контроля защищенности.
29. Требования по обеспечению защиты информации в АИС, классификация АИС.
30. Инвентаризация информационных актив в АИС. Объекты и способы инвентаризации. Инвентаризация информационных актив в АИС с помощью сетевого сканера.
31. Инвентаризация информационных актив в АИС с использованием системных проверок.
32. Уязвимости в АИС и способы их выявления. Понятие уязвимости и категории проверок.
33. Выявление уязвимостей в АИС с использованием тестов и эксплойтов.
34. Выявление уязвимостей в АИС по косвенным признакам.
35. Основные требования нормативно-правовых документов и стандартов в области управления ИБ.
36. Обеспечение ИБ в чрезвычайных ситуациях. План обеспечения управления ИБ предприятия в чрезвычайных ситуациях.



### 5.3. Самостоятельная работа обучающегося.

#### Примерные вопросы и задания для самостоятельной работы студентов

- Риски, связанные с информационными технологиями.
- Нейтрализация (уменьшение, ослабление) рисков. Основные категория безопасности.
- Типовые причины возникновения каналов несанкционированного доступа.
- Действия пользователя информации и злоумышленника, создающие угрозы утечки информации
- Случайный и организованный канал утечки информации. Зависимость вероятности возникновения угрозы воздействия от соотношения цены информации и затрат злоумышленника на ее добывание.
- Основные источники преднамеренных угроз. Основные источники случайных угроз. Опасный функциональный сигнал. Вредоносное программное обеспечение.
- Суть мероприятий по управлению рисками. Процесс интегрирования управления рисками на этапе закупки (разработки) жизненного цикла ИС.
- Процесс интегрирования управления рисками на этапе установки жизненного цикла ИС. Процесс интегрирования управления рисками на этапе эксплуатации жизненного цикла ИС. Процесс интегрирования управления рисками на этапе выведении системы из эксплуатации жизненного цикла ИС.
- Основные объекты инфологической модели объекта Перечень наиболее распространенных угроз. Основные компоненты модели угроз организации.
- Основные источники возникновения угроз. Возможности конкурентов, клиентов, посетителей и хакеров в качестве потенциальных злоумышленников. Цели администраторов, программистов, операторов, руководителей, технического персонала, сотрудников, уволенных с работы в качестве потенциальных нарушителей ИБ
- Модели оценки вероятности осуществления угрозы. Основные метрики, используемые для оценки вероятности осуществления угрозы. Способы предупреждения возможных угроз.
- Способы обнаружения угроз. Способы пресечения или локализации угроз. Действия способа ликвидации последствий.
- Защитные действия при реализации способов ЗИ. Три группы мероприятий по технической защите информации. Основные организационные мероприятия по технической защите информации.
- Роль руководителя организации в процессе управления рисками информационной безопасности. Роль начальника отдела (управления) информационной безопасности в процессе управления рисками информационной безопасности. Этапы процесса управления рисками.
- Этап выбора анализируемых объектов и уровня детализации их рассмотрения процесса управления рисками. Основные шаги анализа угроз в процедуре управления рисками.
- Этап оценки рисков в процедуре управления рисками. Этап выбора защитных мер в процедуре управления рисками. Этап реализации и проверки выбранных мер защиты в процедуре управления рисками.
- Возможности в процессе ограничения (нейтрализации) риска. Возможности в процессе переадресации риска. Оценка экономической эффективности. План реализации контрмер.
- Трактовка и способы вычисления рисков. Представление рисков в виде дерева уязвимостей, угроз и контрмер.

Фонд оценочных материалов (ФОМ) для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом.

## 6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 6.1. Книгообеспеченность

Наименование литературы: автор, название, вид издания, издательство	Год издания	КНИГООБЕСПЕЧЕННОСТЬ
		Наличие в электронном каталоге ЭБС
Основная литература*		
Чекулаева, Е. Н. Управление информационной безопасностью: учебное пособие: [16+] / Е. Н. Чекулаева, Е. С. Кубашева; Поволжский государственный технологический университет. – Йошкар-Ола: Поволжский государственный технологический университет, 2020. – 156 с. ISBN 978-5-8158-2165-1	2020	<a href="https://biblioclub.ru/index.php?page=book&amp;id=612591">https://biblioclub.ru/index.php?page=book&amp;id=612591</a> (дата обращения: 25.08.2021)
Шилов, А. К. Управление информационной безопасностью: учебное пособие: [16+] / А. К. Шилов; Южный федеральный университет, Институт компьютерных технологий и информационной безопасности. – Ростов-на-Дону; Таганрог: Южный федеральный университет, 2018. – 121 с. ISBN 978-5-9275-2742-7	2018	<a href="https://biblioclub.ru/index.php?page=book&amp;id=500065">https://biblioclub.ru/index.php?page=book&amp;id=500065</a> (дата обращения: 25.08.2021)
Абденов, А. Современные системы управления информационной безопасностью: учебное пособие: [16+] / А. Абденов, Г. Дронова, В. Трушин; Новосибирский государственный технический университет. – Новосибирск: Новосибирский государственный технический университет, 2017. – 48 с. ISBN 978-5-7782-3236-5	2017	<a href="https://biblioclub.ru/index.php?page=book&amp;id=574594">https://biblioclub.ru/index.php?page=book&amp;id=574594</a> (дата обращения: 25.08.2021)
Веселов, Г. Е. Менеджмент риска информационной безопасности: учебное пособие / Г. Е. Веселов, Е. С. Абрамов, А. К. Шилов; Южный федеральный университет, Инженерно-технологическая академия. – Таганрог: Южный федеральный университет, 2016. – 109 с. ISBN 978-5-9275-2327-5	2016	<a href="https://biblioclub.ru/index.php?page=book&amp;id=493331">https://biblioclub.ru/index.php?page=book&amp;id=493331</a> (дата обращения: 25.08.2021)
Аверченков, В. И. Аудит информационной безопасности: учебное пособие для вузов / В. И. Аверченков. – 3-е изд., стер. – Москва: ФЛИНТА, 2016. – 269 с. ISBN 978-5-9765-1256-6	2016	<a href="https://biblioclub.ru/index.php?page=book&amp;id=93245">https://biblioclub.ru/index.php?page=book&amp;id=93245</a> (дата обращения: 25.08.2021)
Дополнительная литература		
Аверченков, В. И. Служба защиты информации: организация и управление: [16+] / В. И. Аверченков, М. Ю. Рытов. – 3-е изд., стер. – Москва: ФЛИНТА, 2016. – 186 с. ISBN 978-5-9765-1271-9	2016	<a href="https://biblioclub.ru/index.php?page=book&amp;id=93356">https://biblioclub.ru/index.php?page=book&amp;id=93356</a> (дата обращения: 25.08.2021)
Жукова, М. Н. Управление информационной безопасностью. Ч. 2.: учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. – Красноярск: Сиб. гос. аэрокосмич. ун-т, 2012. – 100 с.	2012	<a href="http://znanium.com/catalog.php?bookinfo=463061">http://znanium.com/catalog.php?bookinfo=463061</a> (дата обращения: 25.08.2021)
Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. – М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. – 592 с.	2013	<a href="http://znanium.com/catalog.php?bookinfo=402686">http://znanium.com/catalog.php?bookinfo=402686</a> (дата обращения: 25.08.2021)

### 6.2. Периодические издания

1. Электронный журнал «Защита информации. Инсайд» ISSN 2413-3582, Режим доступа: <http://inside-zi.ru/pages/about.html>
2. Электронный журнал «Спецтехника и Связь», Режим доступа: <http://www.st-s.ru/>
3. Электронный журнал «Системы безопасности связи и телекоммуникаций» –компания «Гротек», Москва [Электронный ресурс] // URL: <http://sccs.intelgr.com/>
4. Электронный научно-технический журнал «Специальная техника», Москва [Электронный ресурс] // URL: <http://www.ess.ru/>

5. Электронный журнал «БДИ» (Безопасность, Достоверность, Информация), С.-Петербург. [Электронный ресурс] // URL: <http://asbgroup.ru/izdaniya/zhurnal-bdi/>

### **6.3. Интернет-ресурсы**

1. Сайт «Группа СТ» г. Санкт-Петербург [Электронный ресурс] // URL: <http://spymarket.com/>
2. Сайт «Группа компаний «Маском»» г.Москва [Электронный ресурс] // URL: <http://www.mascom.ru/> (дата обращения: 13.06.2018).
3. Сайт ЗАО НПЦ Фирма "НЕЛК" г. Москва [Электронный ресурс] // URL: <https://www.nelk.ru/>
4. Сайт «НПО Защита информации» г. Москва [Электронный ресурс] // URL: <http://www.sinf.ru/>
5. Сайт компании «Проминформзащита» г. Москва [Электронный ресурс] // URL: <http://www.profinfo.ru/>
6. Сайт компании «Сюртель» г. Москва [Электронный ресурс] // URL: <http://www.suritel.ru/>
7. ЗАО ПФ «Элвира» Московская обл. г. Железнодорожный [Электронный ресурс] // URL: <http://www.elvira.ru/>

## **7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

Занятия проводятся в следующих аудиториях ВлГУ (корпус №2) по адресу г. Владимир, ул. Белоконской, д. 3.

ауд. 408-2, Лекционная аудитория, количество студенческих мест – 50, площадь 60 м<sup>2</sup>, оснащение: мультимедийное оборудование (интерактивная доска Hitachi FX-77WD, проектор BenQ MX 503 DLP 2700ANSI XGA), ноутбук Lenovo Idea Pad B5045

ауд. 427а-2, лаборатория сетевых технологий, количество студенческих мест – 14, площадь 36 м<sup>2</sup>, оснащение: компьютерный класс с 8 рабочими станциями Core 2 Duo E8400 с выходом в Internet, 3 маршрутизатора Cisco 2800 Series, 6 маршрутизаторов Cisco 2621, 6 коммутаторов Cisco Catalyst 2960 Series, 3 коммутатора Cisco Catalyst 2950 Series, коммутатор Cisco Catalyst Express 500 Series, проектор BenQ MP 620 P, экран настенный рулонный. Лицензионное программное обеспечение: операционная система Windows 7 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2007, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, программный продукт виртуализации Oracle VM VirtualBox 5.0.4, симулятор сети передачи данных Cisco Packet Tracer 7.0, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 15.0.3.

ауд. 427б-2, УНЦ «Комплексная защита объектов информатизации», количество студенческих мест – 15, площадь 52 м<sup>2</sup>, оснащение: компьютерный класс с 7 рабочими станциями Alliance Optima P4 с выходом в Internet, коммутатор D-Link DGS-1100-16 мультимедийный комплект (проектор Toshiba TLP X200, экран настенный рулонный), прибор ST-031P «Пиранья-Р» многофункциональный поисковый, прибор «Улан-2» поисковый, виброакустический генератор шума «Соната АВ 1М», имитатор работы средств нелегального съема информации, работающих по радиоканалу «Шиповник», анализатор спектра «GoodWill GSP-827», индикатор поля «SEL SP-75 Black Hunter», устройство блокирования работы систем мобильной связи «Мозайка-3», устройство защиты телефонных переговоров от прослушивания «Прокруст 2000», диктофон Edic MINI Hunter, локатор «Родник-2К» нелинейный, комплекс проведения акустических и виброакустических измерений «Спрут мини-А», видеорегистратор цифровой Best DVR-405, генератор Шума «Гном-3», учебно-исследовательский комплекс «Сверхширокополосные беспроводные сенсорные сети» (Nano Chaos), сканирующий приемник «Icom IC-R1500», анализатор сетей Wi-Fi Fluke AirCheck с активной антенной. Лицензионное программное обеспечение: Windows 8 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2010, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, инструмент имитационного моделирования AnyLogic 7.2.0 Personal Learning Edition, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 14.1.4.

Рабочую программу составил доцент кафедры ИЗИ Тельный А.В.

(ФИО, должность, подпись)

Рецензент

(представитель работодателя) Заместитель руководителя РАЦ ООО «ИнфоЦентр»  
к.т.н. Вертилевский Н.В.

(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № \_\_\_\_\_ от \_\_\_\_\_ года

Заведующий кафедрой д.т.н., профессор

/М.Ю. Монахов/

(ФИО, подпись)

Рабочая программа рассмотрена и одобрена

на заседании учебно-методической комиссии специальности 10.05.04 «Информационно-аналитические системы безопасности»

Протокол № \_\_\_\_\_ от \_\_\_\_\_ года

Председатель комиссии д.т.н., профессор

/М.Ю. Монахов/

(ФИО, должность, подпись)

### ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на 20 22 / 20 23 учебный год

Протокол заседания кафедры № 14 от 28.06.14 года

Заведующий кафедрой д.т.н., профессор

/М.Ю. Монахов/

(ФИО, подпись)

Рабочая программа одобрена на 20 \_\_\_\_ / 20 \_\_\_\_ учебный года

Протокол заседания кафедры № \_\_\_\_ от \_\_\_\_ года

Заведующий кафедрой \_\_\_\_\_

Рабочая программа одобрена на 20 \_\_\_\_ / 20 \_\_\_\_ учебный года

Протокол заседания кафедры № \_\_\_\_ от \_\_\_\_ года

Заведующий кафедрой \_\_\_\_\_

**ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ**

в рабочую программу дисциплины

*Основы управления информационной безопасностью*

образовательной программы специальности 10.05.04

«Информационно-аналитические системы безопасности»

Номер изменения	Внесены изменения в части/разделы рабочей программы	Исполнитель ФИО	Основание (номер и дата протокола заседания кафедры)
1			
2			

Заведующий кафедрой \_\_\_\_\_ /М.Ю. Монахов/

*Подпись**ФИО*