

УТВЕРЖДАЮ  
 Декан факультета

\_\_\_\_\_  
 (подпись) Матвеев П.В.  
 ФИО  
 «\_\_\_» \_\_\_\_\_ 20\_\_

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Направление/специальность подготовки	09.03.02 Информационные системы и технологии
Специализация/профиль/программа подготовки	Информационная безопасность
Уровень высшего образования	Бакалавриат
Форма обучения	Очная
Факультет	О Естественнонаучный
Выпускающая кафедра	О7 Информационные системы и программная инженерия
Кафедра-разработчик рабочей программы	О7 Информационные системы и программная инженерия

КУРС	СЕМЕСТР	ОБЩАЯ ТРУДОЁМКОСТЬ (ЗАЧЕТНЫХ ЕДИНИЦ)	ЧАСЫ (по наличию видов занятий)									ВИД ПРОМЕЖУТОЧНОГО КОНТРОЛЯ
			ОБЩАЯ ТРУДОЁМКОСТЬ	АУДИТОРНЫЕ ЗАНЯТИЯ				САМОСТОЯТЕЛЬНАЯ РАБОТА				
				ВСЕГО	ЛЕКЦИИ	ЛАБОРАТОРНЫЙ ПРАКТИКУМ	ПРАКТИЧЕСКИЕ ЗАНЯТИЯ	ВСЕГО	КУРСОВОЙ ПРОЕКТ	КУРСОВАЯ РАБОТА	ДРУГИЕ ВИДЫ САМОСТ. РАБОТЫ	
4	8	3	108	39	26	0	13	69	0	0	69	ЭКЗ.

*ЛИСТ СОГЛАСОВАНИЯ*

РАБОЧАЯ ПРОГРАММА СОСТАВЛЕНА В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ФЕДЕРАЛЬНОГО  
ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ОБРАЗОВАНИЯ (ФГОС ВО)

**09.03.02 Информационные системы и технологии**

год набора группы: 2024

Программу составил:

Кафедра О7 Информационные системы и программная инженерия  
Шимкун Вячеслав Владиславович, старший преподаватель

\_\_\_\_\_

Программа рассмотрена  
на заседании кафедры-разработчика  
рабочей программы **О7 Информационные системы и программная инженерия**

Заведующий кафедрой Семенова Е.Г., д.т.н., проф.

\_\_\_\_\_

Программа рассмотрена  
на заседании выпускающей кафедры

**О7 Информационные системы и программная инженерия**

Заведующий кафедрой Семенова Е.Г., д.т.н., проф.

\_\_\_\_\_

# **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

## **ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ**

### **Разделы рабочей программы**

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО
3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ
5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ
6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### **Приложения к рабочей программе дисциплины**

- Приложение 1. Аннотация рабочей программы
- Приложение 2. Технологии и формы обучения
- Приложение 3. Фонды оценочных средств

## 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование следующих компетенций:

ПСК-2.1 — Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности, принимать участие в проведении экспериментальных исследований системы защиты информации

Формированию компетенций служит достижение следующих результатов образования:

### **ПСК-2.1**

*знания:*

основные меры по защите информации (организационные, правовые, программно-аппаратные, криптографические, технические);

основные методы управления информационной безопасностью;

*умения:*

выполнение планирования, идентификации и анализа рисков;

составление аналитических обзоров по вопросам обеспечения информационной безопасности, моделирование рисков;

*навыки:*

владение специализированным программным обеспечением.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.02 Информационные системы и технологии*.

Содержание дисциплины является логическим продолжением дисциплин: **ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ПРАВОВЕДЕНИЕ, АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ, ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.**

Предварительные компетенции, сформированные у обучающегося до начала изучения дисциплины:

- ОПК-3 — Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
- ПСК-2.1 — Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности, принимать участие в проведении экспериментальных исследований системы защиты информации
- ПСК-2.12 — Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
- ПСК-2.14 — Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности
- ПСК-2.9 — Способность выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности
- УК-10 — Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности
- 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

### 3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч.

#### 3.1. Содержание (дидактика) дисциплины

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме			Самостоятельная работа студентов	Формируемая компетенция, %
				ВСЕГО	Лекции	Практические занятия		ПСК-2.1
4	8	Раздел 1. Анализ объекта защиты. 1.1 Технология анализа объекта защиты. 1.2 Типы информационных систем. 1.3 Методы оценки ущерба от реализации угроз информационной безопасности. 1.4 Комплекс стандартов в области информационной безопасности.	19	8	6	2	11	10
4	8	Раздел 2. Модель угроз и модель нарушителя. 2.1. Подходы к формированию модели нарушителя и модели угроз. 2.2. Требования регуляторов к формированию модели нарушителя и модели угроз.	17	5	3	2	12	10
4	8	Раздел 3. Оценка рисков информационной безопасности. 3.1 Основные положения стандартов в области управления рисками информационной безопасности.	17	6	3	3	11	20
4	8	Раздел 4. Система управления информационной безопасностью. 4.1 Основные положения стандартов по проектированию, реализации и аудиту системы управления информационной безопасностью. 4.2 Организация управления персоналом в контексте обеспечения информационной безопасности.	21	9	7	2	12	20
4	8	Раздел 5. Политика информационной безопасности. 5.1 Основные положения стандартов в области регламентации обеспечения информационной безопасности.	17	5	3	2	12	20
4	8	Раздел 6. Управление инцидентами информационной безопасности. 6.1 Основные положения стандартов в области управления инцидентами информационной безопасности. 6.2 Регламентация действий сотрудников при возникновении нештатных ситуаций.	17	6	4	2	11	20
Всего за 8 семестр			108	39	26	13	69	100
Всего по дисциплине			108	39	26	13	69	100

#### 3.2. Аудиторный практикум

№ п/п	Номер и наименование раздела дисциплины	Тема практического занятия	Объем, ауд. часов
1	Раздел 1. Анализ объекта защиты.	Практическая работа №1 – «Формальное описание структуры информационной системы»	2
2	Раздел 2. Модель угроз и модель нарушителя.	Практическая работа №2 – «Составление модели угроз информационной системе»	2
3	Раздел 3. Оценка рисков информационной безопасности.	Практическая работа №3 – «Анализ рисков информационной безопасности на основе построения модели информационных потоков, анализ рисков на основе модели угроз и уязвимостей, система управления информационной безопасностью»	3
4	Раздел 4. Система управления информационной безопасностью.	Практическая работа №4 – «Формирование требований к системе защиты информации»	2
5	Раздел 5. Политика информационной безопасности.	Практическая работа №5 – «Формирование требований к политике информационной безопасности»	2
6	Раздел 6. Управление инцидентами информационной безопасности.	Практическая работа №6 – «Анализ рисков на основе международного стандарта ISO 17799»	2
Всего за 8 семестр			13

#### 3.3. Самостоятельная работа студента (СРС)

№	Номер и	Содержание учебного задания	Объем,
---	---------	-----------------------------	--------

п/п	наименование раздела дисциплины		часов
1	Раздел 1. Анализ объекта защиты.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	5
2		Подготовка к практической работе №1 – «Формальное описание структуры информационной системы».	6
3	Раздел 2. Модель угроз и модель нарушителя.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	6
4		Подготовка к практической работе №2 – «Составление модели угроз информационной системе».	6
5	Раздел 3. Оценка рисков информационной безопасности.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	5
6		Подготовка к практической работе №3 – «Анализ рисков информационной безопасности на основе построения модели информационных потоков. Анализ рисков на основе модели угроз и уязвимостей. Система управления информационной безопасностью».	6
7	Раздел 4. Система управления информационной безопасностью.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	6
8		Подготовка к практической работе №4 – «Формирование требований к системе защиты информации».	6
9	Раздел 5. Политика информационной безопасности.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	6
10		Подготовка к практической работе №5 – «Формирование требований к политике информационной безопасности».	6
11	Раздел 6. Управление инцидентами информационной безопасности.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	5
12		Подготовка к практической работе №6 – «Анализ рисков на основе международного стандарта ISO 17799».	6
Всего за 8 семестр			69

#### 4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

СЕМЕСТР	НЕДЕЛИ СЕМЕСТРА												
	1	2	3	4	5	6	7	8	9	10	11	12	13
8		Отч. по ПЗ		Отч. по ПЗ		ДР		Отч. по ПЗ		ДР		Отч. по ПЗ	Вопр. Экз

Условные обозначения:

- ДР – диагностическая работа;
- Отч. по ПЗ – отчет по практическому заданию;
- Вопр. Экз – вопросы к экзамену.

**Текущий контроль успеваемости** студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- отчет по практическому заданию;
- вопросы к экзамену.

**Промежуточная аттестация** проводится в формах:

- экзамен.

## 5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 5.1. Основная литература по дисциплине:

1. В. И. Ярочкин. . Информационная безопасность. М.: Академический Проект, 2006, 48 экз.
2. В. Ф. Шаньгин. . Комплексная защита информации в корпоративных системах. М.: Форум, 2010, 5 экз.
3. Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019, 42 экз.
4. Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019, эл. рес.
5. С. А. Нестеров. . Информационная безопасность. Москва: Юрайт, 2019, эл. рес.
6. Ю. А. Родичев. . Информационная безопасность. Национальные стандарты Российской Федерации. Санкт-Петербург: Питер, 2019, эл. рес.
7. Ю. Н. Сычёв. . Стандарты информационной безопасности. Защита и обработка конфиденциальных документов. Москва: ИНФРА-М, 2021, эл. рес.
8. Ю. Ю. Громов, В. О. Драчёв, О. Г. Иванова. . Информационная безопасность и защита информации. Старый Оскол: ТНТ, 2010, 22 экз.

### 5.2. Дополнительная литература по дисциплине:

1. В. Я. Ищейнов, М. В. Мецатунян. . Защита конфиденциальной информации. М.: Форум, 2009, 2 экз.
2. Н. З. Емельянова, Т. Л. Партыка, И. И. Попов. . Защита информации в персональном компьютере. М.: Форум, 2009, 2 экз.

### 5.3. Периодические издания:

не требуются.

### 5.4. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины, электронные библиотечные системы:

1. <http://www.intuit.ru/department/security/secst/> — НОУ ИНТУИТ | Стандарты информационной безопасности | Информация;
2. <http://www.intuit.ru/department/security/secbasics/> — НОУ ИНТУИТ | Основы информационной безопасности | Информация;
3. <http://e.lanbook.com/> — ЭБС Лань;;
4. <https://urait.ru/> — Образовательная платформа «Юрайт». Для вузов и ссузов.;;
5. <http://library.voenmeh.ru/jirbis2/> — Р“Р»Р°РІРРР°СІЃ; — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.

### Современные профессиональные базы данных:

1. <https://rusneb.ru> – Национальная электронная библиотека (НЭБ);
2. <https://cyberleninka.ru/> - Научная электронная библиотека «Киберленинка»;  
<http://www.rfbr.ru/rffi/ru/library> - Полнотекстовая электронная библиотека Российского фонда фундаментальных исследований.

### Информационные справочные системы:

1. Техэксперт – Информационный портал технического регулирования: Нормы, правила, стандарты РФ;
2. [http://library.voenmeh.ru/jirbis2/index.php?option=com\\_irbis&view=irbis&Itemid=457](http://library.voenmeh.ru/jirbis2/index.php?option=com_irbis&view=irbis&Itemid=457) - БД ГОСТов собственной генерации БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова;
3. <http://www.consultant.ru/>- КонсультантПлюс- информационный портал правовой информации.

### 5.5. Программное обеспечение:

не требуется.

### 5.6. Информационные технологии:



взаимодействие с обучающимися посредством ЭИОС Moodle БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.

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

### **6.1. Лекционные занятия:**

специализированные требования по оборудованию отсутствуют; аудитория с посадочными местами по количеству студентов; доска.

### **6.2. Практические занятия:**

специализированные требования по оборудованию отсутствуют; аудитория с посадочными местами по количеству студентов; доска.

### **6.3. Прочее:**

1. рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
2. рабочие места студентов, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде.

### Аннотация рабочей программы

Дисциплина **ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.02 Информационные системы и технологии*. Дисциплина реализуется на факультете *О Естественнотехнический БГТУ "ВОЕНМЕХ"* им. Д.Ф. Устинова кафедрой *О7 Информационные системы и программная инженерия*.

Дисциплина нацелена на формирование *компетенций*:

ПСК-2.1 Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности, принимать участие в проведении экспериментальных исследований системы защиты информации.

Содержание дисциплины охватывает круг вопросов, связанных с управлением информационной безопасностью, методами и средствами ее обеспечения. Рассматриваются системы менеджмента информационной безопасности, требования к органам, осуществляющим аудит и сертификацию данных систем, безопасность сетей, а также методы и средства идентификации, сбора, получения и хранения средств, представленных в цифровой форме.

Программой дисциплины предусмотрены следующие **виды контроля**:

**Текущий контроль успеваемости** студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- отчет по практическому заданию;
- вопросы к экзамену.

**Промежуточная аттестация** проводится в формах:

- экзамен.

Общая трудоемкость освоения дисциплины составляет **3 з.е., 108 ч.** Программой дисциплины предусмотрены лекционные занятия (**26 ч.**), практические занятия (**13 ч.**), самостоятельная работа студента (**69 ч.**).

## ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

### Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 108 ч., из них 39 ч. аудиторных занятий, и 69 ч., отведенных на самостоятельную работу студента.

Рекомендации по распределению учебного времени по видам самостоятельной работы и разделам дисциплины приведены в таблице.

Контроль освоения дисциплины производится в соответствии с Положением о текущем, рубежном контроле успеваемости и промежуточной аттестации обучающихся.

Формы контроля и критерии оценивания приведены в приложении 3 к Рабочей программе.

Наименование работы	Рекомендуемая литература	Трудоемкость, час.
<b>Раздел 1. Анализ объекта защиты.</b>		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	В. Ф. Шаньгин. . Комплексная защита информации в корпоративных системах: М.: Форум, 2010 (1) Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (1) В. И. Ярочкин. . Информационная безопасность: М.: Академический Проект, 2006 (1) Н. З. Емельянова, Т. Л. Партыка, И. И. Попов. . Защита информации в персональном компьютере: М.: Форум, 2009 (1)	5
Подготовка к практической работе №1 – «Формальное описание структуры информационной системы».	В. Я. Ищейнов, М. В. Мецатунян. . Защита конфиденциальной информации: М.: Форум, 2009 (1) Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (1)	6
Итого по разделу 1		11
<b>Раздел 2. Модель угроз и модель нарушителя.</b>		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	В. Ф. Шаньгин. . Комплексная защита информации в корпоративных системах: М.: Форум, 2010 (2) Н. З. Емельянова, Т. Л. Партыка, И. И. Попов. . Защита информации в персональном компьютере: М.: Форум, 2009 (2)	6
Подготовка к практической работе №2 – «Составление модели угроз информационной системе».	Ю. А. Родичев. . Информационная безопасность.	6

	Национальные стандарты Российской Федерации: Санкт-Петербург: Питер, 2019 (2) В. И. Ярочкин. . Информационная безопасность: М.: Академический Проект, 2006 (2)	
Итого по разделу 2		12
<b>Раздел 3. Оценка рисков информационной безопасности.</b>		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	В. Ф. Шаньгин. . Комплексная защита информации в корпоративных системах: М.: Форум, 2010 (3) Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (2-3)	5
Подготовка к практической работе №3 – «Анализ рисков информационной безопасности на основе построения модели информационных потоков. Анализ рисков на основе модели угроз и уязвимостей. Система управления информационной безопасностью».	Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (2-3) В. И. Ярочкин. . Информационная безопасность: М.: Академический Проект, 2006 (2-3) Ю. Н. Сычёв. . Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: Москва: ИНФРА-М, 2021 (1-3)	6
Итого по разделу 3		11
<b>Раздел 4. Система управления информационной безопасностью.</b>		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	В. Ф. Шаньгин. . Комплексная защита информации в корпоративных системах: М.: Форум, 2010 (3-5) Н. З. Емельянова, Т. Л. Партыка, И. И. Попов. . Защита информации в персональном компьютере: М.: Форум, 2009 (3)	6
Подготовка к практической работе №4 – «Формирование требований к системе защиты информации».	В. Я. Ищейнов, М. В. Мецатунян. . Защита конфиденциальной информации: М.: Форум, 2009 (3-4) Ю. А. Родичев. . Информационная безопасность. Национальные стандарты Российской Федерации: Санкт-Петербург: Питер, 2019 (3)	6
Итого по разделу 4		12
<b>Раздел 5. Политика информационной безопасности.</b>		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	С. А. Нестеров. . Информационная безопасность: Москва: Юрайт, 2019 (5)	6
Подготовка к практической работе №5 – «Формирование требований к политике информационной безопасности».	Ю. А. Родичев. . Информационная безопасность. Национальные стандарты Российской Федерации: Санкт-	6

	<p>Петербург: Питер, 2019 (5-6)</p> <p>Ю. Ю. Громов, В. О. Драчёв, О. Г. Иванова. . Информационная безопасность и защита информации: Старый Оскол: ТНТ, 2010 (4-6)</p>	
Итого по разделу 5		12
<b>Раздел 6. Управление инцидентами информационной безопасности.</b>		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	<p>В. Я. Ищeyнов, М. В. Мецатунян. . Защита конфиденциальной информации: М.: Форум, 2009 (5-8)</p> <p>Ю. Ю. Громов, В. О. Драчёв, О. Г. Иванова. . Информационная безопасность и защита информации: Старый Оскол: ТНТ, 2010 (8)</p>	5
Подготовка к практической работе №6 – «Анализ рисков на основе международного стандарта ISO 17799».	<p>Ю. А. Родичев. . Информационная безопасность. Национальные стандарты Российской Федерации: Санкт-Петербург: Питер, 2019 (5-8)</p> <p>В. Ф. Шаньгин. . Комплексная защита информации в корпоративных системах: М.: Форум, 2010 (5-8)</p>	6
Итого по разделу 6		11

## **ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**

Фонд оценочных средств, позволяющие оценить результаты обучения по данной дисциплине, включают в себя:

- диагностическая работа
- отчет по практическому заданию;
- вопросы к экзамену;
- экзамен.

### **Критерии оценивания**

#### **Диагностическая работа**

Диагностическая работа проводится в форме теста в ЭИОС Moodle:

- при правильном ответе менее чем на 60% вопросов - не аттестация;
- при правильном ответе на 60% вопросов и более - аттестация.

#### **Отчет по практическому заданию**

При подготовке к выполнению практических заданий рекомендуется повторить теоретические сведения по теме данной работы в соответствии с указаниями в таблице Приложения 3 к настоящей рабочей программе. При подготовке к защите рекомендуется подготовить ответы на контрольные вопросы по теме данной работы. В случаях затруднений обращаться к преподавателю на очередном практическом занятии или на консультации.

К каждому ПЗ необходимо подготовить отчет в электронном виде. После выполнения отчета его необходимо предоставить на проверку преподавателю (либо лично, либо посредством электронной почты). При выполнении отчета руководствоваться ГОСТ 7.32-2017. Состав отчета описывается в постановке задачи каждого ПЗ.

ПЗ считается выполненным и защищенным успешно при условии:

- наличия корректного решения поставленной задачи;
- наличия отчета;
- защиты ПЗ по комплекту тестовых вопросов для защиты ПЗ, размещенного в УМК дисциплины.

Критерии оценивания:

- соответствие решения указанным требованиям, его работоспособность и эффективность – 7 баллов;
- отчет оформлен полностью в соответствии с ГОСТ 7.32-2017 – 3 балла;
- правильность ответов на вопросы – 7 баллов;
- своевременность выполнения и защиты индивидуального задания – 3 балла.

Основанием для снижения количества баллов являются:

- несоответствие решения указанным требованиям, его неэффективность или некорректная работа;
- оформление отчета не соответствует ГОСТ 7.32-2017 в 3 и более пунктах;
- неверные ответы на вопросы или отсутствие ответов;
- несвоевременность выполнения и защиты индивидуального задания.

В случае, если ПЗ и отчет к нему выполнены своевременно в соответствии с указанными требованиями, а также получены правильные ответы на вопросы при его защите студент получает максимальное количество баллов – 20. Для того, чтобы ПЗ было сдано, требуется набрать 12 баллов.

#### **Вопросы к экзамену**

Вопросы к экзамену содержатся в УМК дисциплины.

При подготовке ответов на теоретические вопросы рекомендуется помимо текстов лекций использовать источники основной и дополнительной литературы.

#### **Экзамен**

Перечень теоретических вопросов к экзамену, представленный в УМК дисциплины, предоставляется преподавателем. Задачи соответствуют программе практических занятий. При подготовке ответов на теоретические вопросы рекомендуется помимо текстов лекций использовать источники основной и дополнительной литературы. Особое внимание следует уделить подготовке практических примеров к теоретическим экзаменационным вопросам.

На экзамене студенту предлагается два теоретических вопроса. При успешном ответе на оба вопроса выставляется оценка «отлично». При ответе на один из двух предложенных вопросов преподавателем может быть выставлена оценка «хорошо» при успешном выполнении всех практических заданий. При отсутствии успешных ответов зачет может быть оформлен с оценкой «удовлетворительно» на основании успешного выполнения предусмотренных рабочей программой практических заданий. При несвоевременном или неполном выполнении практических заданий и при неуспешной сдаче экзамена выставляется оценка «не зачтено».



Паспорт фонда оценочных средств

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме			Самостоятельная работа студентов	Формируемая компетенция, %	НАИМЕНОВАНИЕ ОЦЕНОЧНОГО СРЕДСТВА
				ВСЕГО	Лекции	Практические занятия		ПСК-2.1	
4	8	Раздел 1. Анализ объекта защиты.	19	8	6	2	11	10	Отчет по практическому заданию
4	8	Раздел 2. Модель угроз и модель нарушителя.	17	5	3	2	12	10	Отчет по практическому заданию
4	8	Раздел 3. Оценка рисков информационной безопасности.	17	6	3	3	11	20	Отчет по практическому заданию
4	8	Раздел 4. Система управления информационной безопасностью.	21	9	7	2	12	20	Отчет по практическому заданию
4	8	Раздел 5. Политика информационной безопасности.	17	5	3	2	12	20	Отчет по практическому заданию
4	8	Раздел 6. Управление инцидентами информационной безопасности.	17	6	4	2	11	20	Отчет по практическому заданию, Вопросы к экзамену
Всего за 8 семестр			108	39	26	13	69	100	
Всего по дисциплине			108	39	26	13	69	100	

## Критерии оценивания

### ПСК-2.1

*Вопросы открытого типа:*

- № 1 Что такое **управление информационной безопасностью**?
- № 2 Что такое **система**?
- № 3 Что понимается под **системным подходом**?
- № 4 Что такое **процесс**?
- № 5 Что подразумевается под **процессным подходом**?
- № 6 Что представляет собой **управление**?
- № 7 Что такое **объект управления**?
- № 8 Дайте определение термину "**метод управления**".
- № 9 Что представляет собой **программное управление**?
- № 10 Что такое **техническая политика информационной безопасности**?

*Вопросы закрытого типа:*

- № 1 **Процесс** (от лат. *processus* – продвижение) – это:
  - 1) последовательная смена явлений, состояний в развитии чего-нибудь;
  - 2) цепь логически связанных, повторяющихся действий, в результате которых используются ресурсы организации с целью достижения определенных измеримых результатов для удовлетворения внутренних или внешних потребителей;
  - 3) статистическая обработка результатов моделирования;
  - 4) поиск и оценка альтернативных решений;
  - 5) формулирование выводов и предложений по решению проблемы;
  - 6) всё перечисленное.
- № 2 Расставьте в правильном порядке элементы циклической модели улучшения процессов:
  - действуй (усвой изменения или отбрось их, или повтори ещё раз при других условиях);
  - проверяй, оценивай, изучай результат;
  - планируй изменения или испытания, направленные на улучшение;
  - попробуй осуществить.
- № 3 Какой стандарт (серия стандартов) стал основоположником стандартизации систем управления информационной безопасностью?
  - 1) ISO 9000
  - 2) ISO/IEC 27000
  - 3) BS 7799:1995
  - 4) BS 77991:1999
  - 5) ISO/IEC 17799:2000
  - 6) ISO/IEC 17799:2005
- № 4 Для организаций какой сферы применимы стандарты серии **ISO/IEC 27000**?
  - 1) Управление информационной безопасностью в финансовом секторе
  - 2) Управление информационной безопасностью в страховом секторе
  - 3) Управление информационной безопасностью в различных сферах деятельности

- 4) Управление информационной безопасностью в сфере здравоохранения
- 5) Управление информационной безопасностью в сфере телекоммуникаций
- № 5 **Политика информационной безопасности организации** - это ...
- 1) Совокупность требований и правил по обеспечению информационной безопасности для объекта информационной безопасности, выработанных в соответствии с требованиями руководящих и нормативных документов в целях противодействия заданному множеству угроз информационной безопасности, с учетом ценности защищаемой информационной сферы и стоимости системы обеспечения информационной безопасности.
- 2) Документированные решения в области обеспечения информационной безопасности.
- 3) Совокупность (одно или несколько) документированных правил, процедур, практических приемов в области безопасности, которыми руководствуется организация в своей деятельности.
- 4) Всё перечисленное.
- 5) Ничто из перечисленного.
- № 6 Как называют политику информационной безопасности, ориентированную на отдельную область обеспечения информационной безопасности или технологию, используемую в организации или ее подразделении?
- 1) Частная политика информационной безопасности.
- 2) Политика информационной безопасности по конкретным вопросам.
- 3) Политика информационной безопасности по конкретным проблемам.
- 4) Политика информационной безопасности по конкретным системам.
- 5) Любой из перечисленных вариантов.
- № 7 Выберите три основных **трастовых модели** на которых может быть основана **политика информационной безопасности**:
- 1) Либеральная.
- 2) Бескомпромиссная.
- 3) Запретительная.
- 4) Авторитарная.
- 5) Компромиссная.
- 6) Разрешительная.
- 7) Унитарная.
- 8) Открытая.
- № 8 Какой современный **ГОСТ** описывает общее содержание комплексной (корпоративной) **политики информационной безопасности**?
- 1) ГОСТ Р ИСО 9000-2001
- 2) ГОСТ Р ИСО/МЭК 17799-2005
- 3) ГОСТ Р 50922-2006
- 4) ГОСТ Р 53113.1-2008
- № 9 По каким причинам **политика информационной безопасности** может быть **аннулирована**?

- 1) Политика информационной безопасности достигла заключительной стадии и должна быть изъята из обращения, чтобы избежать путаницы.
- 2) Политика информационной безопасности не в полной мере отвечает всем потребностям организации.
- 3) Организация больше не применяет технологию, для которой разрабатывалась политика информационной безопасности.
- 4) Пункты 2 и 3.
- 5) Пункты 1, 2 и 3.
- № 10 Какой **ГОСТ** определяет этапы **управления информационной безопасностью** информационно-телекоммуникационных технологий организации?
- 1) ГОСТ Р ИСО/МЭК 133351
- 2) ГОСТ Р ИСО/МЭК 17799-2005
- 3) ГОСТ Р 50922-2006
- 4) ГОСТ Р 53113.1-2008
- 5) ГОСТ Р ИСО/МЭК ТО 133353