**Министерство науки и высшего образования Российской Федерации**
**Федеральное государственное автономное образовательное учреждение высшего образования**
**«Самарский государственный экономический университет»**

**Институт** Институт экономики предприятий

**Кафедра** Прикладной информатики

**УТВЕРЖДЕНО**
Ученым советом Университета
(протокол № 11 от 30 мая 2023 г. )

# РАБОЧАЯ ПРОГРАММА

**Наименование дисциплины** Б1.В.12 Организационная защита информации

**Основная профессиональная образовательная программа** 09.03.03 Прикладная информатика программа Прикладная информатика и защита информации

Квалификация (степень) выпускника Бакалавр

Самара 2023

**Содержание (рабочая программа)**

Стр.


1 Место дисциплины в структуре ОП

2 Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе

3 Объем и виды учебной работы

4 Содержание дисциплины

5 Материально-техническое и учебно-методическое обеспечение дисциплины

6 Фонд оценочных средств по дисциплине

Целью изучения дисциплины является формирование результатов обучения, обеспечивающих достижение планируемых результатов освоения образовательной программы.

**1. Место дисциплины в структуре ОП**

Дисциплина Организационная защита информации входит в часть, формируемая участниками образовательных отношений блока Б1.Дисциплины (модули)

Предшествующие дисциплины по связям компетенций: Хранение, обработка и анализ данных, Вычислительные системы, сети и телекоммуникации, Основы алгоритмизации и программирования, Основы проектной деятельности, Современные технологии и языки программирования, Теория информационной безопасности и методология защиты информации, Системы искусственного интеллекта, Облачные технологии и услуги, Технологии защищенного документооборота, Правовая защита информации, Методы и средства защиты информации, Информационно-коммуникационные технологии в профессиональной деятельности, Встроенные языки программирования, Организация вычислительных процессов, Технологии работы в социальных сетях

Последующие дисциплины по связям компетенций: Разработка профессиональных приложений, Проектный практикум, Проектирование информационных систем, Управление информационной безопасностью, Специализированные ИТ в правоохранительной деятельности, Управление информационными проектами реализации комплексной безопасности, Цифровая культура в профессиональной деятельности, Интеллектуальные информационные системы, Современные цифровые технологии управления предприятием

**2. Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе**

Изучение дисциплины Организационная защита информации в образовательной программе направлено на формирование у обучающихся следующих компетенций:

**Профессиональные компетенции (ПК):**

ПК-1 - Способен к обнаружению и идентификации инцидентов в процессе эксплуатации автоматизированной системы

| Планируемые результаты обучения по программе | **Планируемые результаты обучения по дисциплине** | | |
|---|---|---|---|
| ПК-1 | ПК-1.1: Знать: | ПК-1.2: Уметь: | ПК-1.3: Владеть (иметь навыки): |
| | особенности инцидентов в процессе эксплуатации автоматизированной системы | обнаруживать и идентифицировать инциденты в процессе эксплуатации автоматизированной системы | навыками обнаружения и идентификации инцидентов в процессе эксплуатации автоматизированной системы |

ПК-2 - Способен к оценке защищенности автоматизированных систем с помощью типовых программных средств

| Планируемые результаты обучения по программе | **Планируемые результаты обучения по дисциплине** | | |
|---|---|---|---|
| ПК-2 | ПК-2.1: Знать: | ПК-2.2: Уметь: | ПК-2.3: Владеть (иметь навыки): |
| | особенности защиты автоматизированных систем с помощью | оценивать защищенность автоматизированных систем с помощью | навыками защищенности автоматизированных систем с помощью типовых программных средств |

| | | | |
|---|---|---|---|
| | типовых программных средств | типовых программных средств | |

ПК-3 - Способен к составлению комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе

| Планируемые результаты обучения по программе | **Планируемые результаты обучения по дисциплине** | | |
|---|---|---|---|
| ПК-3 | ПК-3.1: Знать: | ПК-3.2: Уметь: | ПК-3.3: Владеть (иметь навыки): |
| | особенности составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе | составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе | навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе |

ПК-4 - Способен к анализу изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации

| Планируемые результаты обучения по программе | **Планируемые результаты обучения по дисциплине** | | |
|---|---|---|---|
| ПК-4 | ПК-4.1: Знать: | ПК-4.2: Уметь: | ПК-4.3: Владеть (иметь навыки): |
| | основные угрозы безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации | анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации | навыками анализа изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации |

**3. Объем и виды учебной работы**

Учебным планом предусматриваются следующие виды учебной работы по дисциплине:

**Очная форма обучения**

| **Виды учебной работы** | Всего час/ з.е. |
|---|---|
| | Сем 6 |
| Контактная работа, в том числе: | 74.3/2.06 |
| Занятия лекционного типа | 36/1 |
| Лабораторные работы (лабораторный практикум) | 36/1 |
| Индивидуальная контактная работа (ИКР) | 0.3/0.01 |
| Групповая контактная работа (ГКР) | 2/0.06 |
| Самостоятельная работа: | 35.7/0.99 |
| Промежуточная аттестация | 34/0.94 |
| Вид промежуточной аттестации:<br>Экзамен | <br>Экз |
| Общая трудоемкость (объем части образовательной программы): Часы<br>Зачетные единицы | 144<br>4 |

**заочная форма**

| **Виды учебной работы** | Всего час/ з.е. |
|---|---|
| | Сем 7 |

| | |
|---|---|
| Контактная работа, в том числе: | 6.3/0.18 |
| Занятия лекционного типа | 2/0.06 |
| Лабораторные работы (лабораторный практикум) | 2/0.06 |
| Индивидуальная контактная работа (ИКР) | 0.3/0.01 |
| Групповая контактная работа (ГКР) | 2/0.06 |
| Самостоятельная работа: | 103.7/2.88 |
| Промежуточная аттестация | 34/0.94 |
| Вид промежуточной аттестации:<br>Экзамен | Экз |
| Общая трудоемкость (объем части образовательной программы): Часы<br>Зачетные единицы | 144<br>4 |

**4. Содержание дисциплины**

***4.1. Разделы, темы дисциплины и виды занятий:***

Тематический план дисциплины Организационная защита информации представлен в таблице.

**Разделы, темы дисциплины и виды занятий**
**Очная форма обучения**

| № п/п | Наименование темы (раздела) дисциплины | Контактная работа | | | | Самостоятельная работа | Планируемые результаты обучения в соотношении с результатами обучения по образовательной программе |
|---|---|---|---|---|---|---|---|
| | | Лекции | Занятия семинарского типа / Лаборат. работы | ИКР | ГКР | | |
| 1. | Основные понятия теории защиты информациии. Задачи защиты информации. | 18 | 18 | 0,1 | 1 | 15 | ПК-1.1, ПК-1.2, ПК -1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК- 3.1, ПК-3.2, ПК- 3.3, ПК-4.1, ПК- 4.2, ПК-4.3 |
| 2. | Информация как объект защиты. Государственная политика информационной безопасности. Концепция комплексного обеспечения защиты информации. | 18 | 18 | 0,2 | 1 | 35,7 | ПК-1.1, ПК-1.2, ПК -1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК- 3.1, ПК-3.2, ПК- 3.3, ПК-4.1, ПК- 4.2, ПК-4.3 |
| | Контроль | 34 | | | | | |
| | **Итого** | **36** | **36** | **0.3** | **2** | **35.7** | |

**заочная форма**

| № п/п | Наименование темы (раздела) дисциплины | Контактная работа | | | | Самостоятельная работа | Планируемые результаты обучения в соотношении с результатами обучения по образовательной программе |
|---|---|---|---|---|---|---|---|
| | | Лекции | Занятия семинарского типа / Лаборат. работы | ИКР | ГКР | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1. | Основные понятия теории защиты информациии. Задачи защиты информации. | 1 | | 0,1 | 1 | 50 | ПК-1.1, ПК-1.2, ПК -1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК- 3.1, ПК-3.2, ПК- 3.3, ПК-4.1, ПК- 4.2, ПК-4.3 |
| 2. | Информация как объект защиты. Государственная политика информационной безопасности. Концепция комплексного обеспечения защиты информации. | 1 | 2 | 0,2 | 1 | 53,7 | ПК-1.1, ПК-1.2, ПК -1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК- 3.1, ПК-3.2, ПК- 3.3, ПК-4.1, ПК- 4.2, ПК-4.3 |
| | Контроль | 34 | | | | | |
| | **Итого** | **2** | **2** | 0.3 | 2 | **103.7** | |

### *4.2 Содержание разделов и тем*

#### 4.2.1 Контактная работа

**Тематика занятий лекционного типа**

| №п/п | Наименование темы (раздела) дисциплины | Вид занятия лекционного типа* | Тематика занятия лекционного типа |
|---|---|---|---|
| 1. | Основные понятия теории защиты информациии. Задачи защиты информации. | лекция | Основные понятия теории информационной безопасности. Защита информации в России |
| | | лекция | Предметная область теории защиты информации. |
| | | лекция | Систематизация понятий в области защиты информации. |
| | | лекция | Основные термины и определения правовых понятий |
| | | лекция | Понятия предметной области «защита информации». Понятия, связанные с организацией защиты информации |
| | | лекция | Основные принципы построения систем защиты. |
| | | лекция | Концепция комплексной защиты информации. |
| | | лекция | Задачи защиты информации. |
| | | лекция | Средства реализации комплексной защиты информации |
| 2. | Информация как объект защиты. Государственная политика информационной безопасности. Концепция комплексного обеспечения защиты информации. | лекция | Информация как объект защиты. Понятие об информации как объекте защиты. Уровни представления информации. Основные свойства защищаемой информации. Виды и формы представления информации. |
| | | лекция | Информационные ресурсы. Структура и шкала ценности информации. Классификация информационных ресурсов. Правовой режим информационных ресурсов |
| | | лекция | Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности. |

| | | | |
|---|---|---|---|
| | | лекция | Структура государственной системы защиты информации. Угрозы информационной безопасности |
| | | лекция | Основные направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы |
| | | лекция | Формирование требований к построению безопасности системы |
| | | лекция | Построение безопасных отказоустойчивых систем защиты информации повышенного уровня защиты информации |
| | | лекция | Построение безопасных отказоустойчивых систем |
| | | лекция | Проектирование систем защиты информации |

*лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях, обучающимся

**Тематика занятий семинарского типа**

| №п/п | Наименование темы (раздела) дисциплины | Вид занятия семинарского типа** | Тематика занятия семинарского типа |
|---|---|---|---|
| 1. | Основные понятия теории защиты информациии. Задачи защиты информации. | лабораторные работы | Работа в одноранговой сети Windows |
| | | лабораторные работы | Основные нормативные руководящие документы информационной безопасности. Справочно-правовая система «Консультант Плюс» |
| | | лабораторные работы | Основные нормативные руководящие документы информационной безопасности. Справочно-правовая система «ГАРАНТ-Максимум |
| | | лабораторные работы | Стандарты информационного обмена |
| | | лабораторные работы | Работа с антивирусными программами |
| | | лабораторные работы | Программная реализация криптографических алгоритмов (Симметричные криптосистемы- шифр перестановки) |
| | | лабораторные работы | Программная реализация криптографических алгоритмов (алгоритмы двойных перестановок) |
| | | лабораторные работы | Программная реализация криптографических алгоритмов(Шифры простой замены) |
| | | лабораторные работы | Программная реализация криптографических алгоритмов(Шифры сложной замены) |
| 2. | Информация как объект защиты. Государственная политика информационной безопасности. Концепция комплексного | лабораторные работы | Асимметричные криптосистемы. |
| | | лабораторные работы | Механизмы контроля целостности данных создать ЭЦП шифрованием профиля сообщения закрытым ключом |
| | | лабораторные работы | Механизмы контроля целостности данных создание профиля дешифрованием ЭЦП открытым ключом отправителя |

| | | | |
|---|---|---|---|
| | обеспечения защиты информации. | лабораторные работы | Защита документов MS Office |
| | | лабораторные работы | Проект «Подготовка документов для разработки проекта политики и программы информационной безопасности предприятия» |
| | | лабораторные работы | Задание 1 «Классификация угроз» |
| | | лабораторные работы | Задание 2 «Нормативно-методическое обеспечение СУИБ». |
| | | лабораторные работы | Задание 3 «Требования к кандидату на должность начальника службы безопасности коммерческой фирмы» |
| | | лабораторные работы | Задание 4 «Управление инцидентами ИБ» |

** семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия

**Иная контактная работа**

При проведении учебных занятий СГЭУ обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Формы и методы проведения иной контактной работы приведены в Методических указаниях по основной профессиональной образовательной программе.

**4.2.2 Самостоятельная работа**

| №п/п | Наименование темы (раздела) дисциплины | Вид самостоятельной работы *** |
|---|---|---|
| 1. | Основные понятия теории защиты информациии. Задачи защиты информации. | - подготовка доклада<br>- подготовка электронной презентации<br>- тестирование |
| 2. | Информация как объект защиты. Государственная политика информационной безопасности. Концепция комплексного обеспечения защиты информации. | - подготовка доклада<br>- подготовка электронной презентации<br>- тестирование |

*** самостоятельная работа в семестре, написание курсовых работ, докладов, выполнение контрольных работ

## 5. Материально-техническое и учебно-методическое обеспечение дисциплины

### 5.1 Литература:

**Основная литература**

1. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511998

2. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2023. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511138

**Дополнительная литература**

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2023. — 104 с. — (Высшее

образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/520063

**5.2. Перечень лицензионного программного обеспечения**

1. Microsoft Windows 10 Education / Microsoft Windows 7 / Windows Vista Business
2. Microsoft Office 2016 Professional Plus (Word, Excel, Access, PowerPoint, Outlook, OneNote, Publisher) / Microsoft Office 2007 (Word, Excel, Access, PowerPoint)

**5.3 Современные профессиональные базы данных, к которым обеспечивается доступ обучающихся**

1. Научная электронная библиотека eLIBRARY.RU https://elibrary.ru/
2. Электронная библиотечная система Юрайт Издательство Юрайт https://biblio-online.ru/
3. Платформа «Библиокомплектатор» http://www.bibliocomplectator.ru/

**5.4. Информационно-справочные системы, к которым обеспечивается доступ обучающихся**

1. Справочно-правовая система «Консультант Плюс»
2. Справочно-правовая система «ГАРАНТ-Максимум»

**5.5. Специальные помещения**

| | |
|---|---|
| Учебные аудитории для проведения занятий лекционного типа | Комплекты ученической мебели<br>Мультимедийный проектор<br>Доска<br>Экран |
| Учебные аудитории для проведения практических занятий (занятий семинарского типа) | Комплекты ученической мебели<br>Мультимедийный проектор<br>Доска<br>Экран<br>Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ |
| Учебные аудитории для групповых и индивидуальных консультаций | Комплекты ученической мебели<br>Мультимедийный проектор<br>Доска<br>Экран<br>Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ |
| Учебные аудитории для текущего контроля и промежуточной аттестации | Комплекты ученической мебели<br>Мультимедийный проектор<br>Доска<br>Экран<br>Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ |
| Помещения для самостоятельной работы | Комплекты ученической мебели<br>Мультимедийный проектор<br>Доска<br>Экран<br>Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ |
| Помещения для хранения и профилактического обслуживания оборудования | Комплекты специализированной мебели для хранения оборудования |

**5.6 Лаборатории и лабораторное оборудование**

| | |
|---|---|
| Лаборатория | Комплекты ученической мебели<br>Мультимедийный проектор<br>Доска<br>Экран<br>Компьютеры с выходом в сеть «Интренет» и ЭИОС СГЭУ<br>Лабораторное оборудование |

**6. Фонд оценочных средств по дисциплине Организационная защита информации:**

**6.1. Контрольные мероприятия по дисциплине**

| **Вид контроля** | **Форма контроля** | **Отметить нужное знаком « + »** |
|---|---|---|
| Текущий контроль | Тестирование | + |
| | Практические задачи | + |
| Промежуточный контроль | Экзамен | + |

**Порядок проведения мероприятий текущего и промежуточного контроля определяется Методическими указаниями по основной профессиональной образовательной программе высшего образования; Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном автономном образовательном учреждении высшего образования «Самарский государственный экономический университет».**

**6.2. Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе**

**Профессиональные компетенции (ПК):**

ПК-1 - Способен к обнаружению и идентификации инцидентов в процессе эксплуатации автоматизированной системы

| Планируемые результаты обучения по программе | **Планируемые результаты обучения по дисциплине** | | |
|---|---|---|---|
| | ПК-1.1: Знать: | ПК-1.2: Уметь: | ПК-1.3: Владеть (иметь навыки): |
| | особенности инцидентов в процессе эксплуатации автоматизированной системы | обнаруживать и идентифицировать инциденты в процессе эксплуатации автоматизированной системы | навыками обнаружения и идентификации инцидентов в процессе эксплуатации автоматизированной системы |
| Пороговый | особенности инцидентов | обнаруживать и идентифицировать инциденты | навыками обнаружения и идентификации инцидентов |
| Стандартный (в дополнение к пороговому) | особенности инцидентов в процессе эксплуатации автоматизированной системы | особенности инцидентов в процессе эксплуатации автоматизированной системы | навыками обнаружения и идентификации инцидентов в процессе эксплуатации автоматизированной системы |

| | | | |
|---|---|---|---|
| Повышенный (в дополнение к пороговому, стандартному) | особенности инцидентов в процессе эксплуатации автоматизированной системы и возможности не допущения инцидентов в процессе эксплуатации автоматизированной системы | особенности инцидентов в процессе эксплуатации автоматизированной системы и их обнаружение | навыками обнаружения и идентификации инцидентов в процессе эксплуатации автоматизированной системы |

ПК-2 - Способен к оценке защищенности автоматизированных систем с помощью типовых программных средств

| Планируемые результаты обучения по программе | **Планируемые результаты обучения по дисциплине** | | |
|---|---|---|---|
| | ПК-2.1: Знать: | ПК-2.2: Уметь: | ПК-2.3: Владеть (иметь навыки): |
| | особенности защиты автоматизированных систем с помощью типовых программных средств | оценивать защищенность автоматизированных систем с помощью типовых программных средств | навыками защищенности автоматизированных систем с помощью типовых программных средств |
| Пороговый | особенности защиты автоматизированных систем | оценивать защищенность автоматизированных систем | навыками защищенности автоматизированных систем |
| Стандартный (в дополнение к пороговому) | особенности защиты автоматизированных систем с помощью типовых программных средств | оценивать защищенность автоматизированных систем с помощью типовых программных средств | навыками защищенности автоматизированных систем с помощью типовых программных средств |
| Повышенный (в дополнение к пороговому, стандартному) | особенности защиты автоматизированных систем с помощью дополнительных программных средств | оценивать защищенность автоматизированных систем с помощью дополнительных программных средств | навыками защищенности автоматизированных систем с помощью дополнительных программных средств |

ПК-3 - Способен к составлению комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе

| Планируемые результаты обучения по программе | **Планируемые результаты обучения по дисциплине** | | |
|---|---|---|---|
| | ПК-3.1: Знать: | ПК-3.2: Уметь: | ПК-3.3: Владеть (иметь навыки): |
| | особенности составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе | составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе | навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе |
| Пороговый | особенности составления комплекса правил | составлять комплекс правил обеспечения | навыками составления комплекса правил |

| | | | |
|---|---|---|---|
| | обеспечения защиты информации в автоматизированной системе | защиты информации в автоматизированной системе | обеспечения защиты информации в автоматизированной системе |
| Стандартный (в дополнение к пороговому) | особенности составления комплекса правил, процедур, практических приемов, принципов и методов защиты информации в автоматизированной системе | составлять комплекс правила и процедуры практических приемов и методов защиты информации в автоматизированной системе | практическими приемами и методами обеспечения защиты информации |
| Повышенный (в дополнение к пороговому, стандартному) | особенности составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе | составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе | навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе |

ПК-4 - Способен к анализу изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации

| Планируемые результаты обучения по программе | **Планируемые результаты обучения по дисциплине** | | |
|---|---|---|---|
| | ПК-4.1: Знать: | ПК-4.2: Уметь: | ПК-4.3: Владеть (иметь навыки): |
| | основные угрозы безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации | анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации | навыками анализа изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации |
| Пороговый | методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; | устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; | навыками установки, настройки программных средств защиты информации в автоматизированной системе; |
| Стандартный (в дополнение к пороговому) | типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации | устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; | тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программноаппаратных средств защиты информации |
| Повышенный (в дополнение к пороговому, стандартному) | типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от | диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных | навыками решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных |

| | | | |
|---|---|---|---|
| | несанкционированного доступа. | средств защиты информации; | средств защиты информации; |

**6.3. Паспорт оценочных материалов**

| № п/п | Наименование темы (раздела) дисциплины | Контролируемые планируемые результаты обучения в соотношении с результатами обучения по программе | Вид контроля/используемые оценочные средства | |
|---|---|---|---|---|
| | | | Текущий | Промежуточный |
| 1. | Основные понятия теории защиты информациии. Задачи защиты информации. | ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-4.3 | Практические задания Тестирование | Экзамен |
| 2. | Информация как объект защиты. Государственная политика информационной безопасности. Концепция комплексного обеспечения защиты информации. | ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-4.3 | Практические задания Тестирование | Экзамен |

**6.4.Оценочные материалы для текущего контроля**

Ссылка на текущую академическую активность, точки текущего контроля для всех оценочных материалов, размещенных в БРСО ЭИОС СГЭУ: https://lms2.sseu.ru/course/index.php?categoryid=1918

**Примерная тематика докладов**

| Раздел дисциплины | Темы |
|---|---|
| Основные понятия теории защиты информациии. Задачи защиты информации. | 1. Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними<br>2. Современные средства защиты информации<br>3. Современные системы компьютерной безопасности<br>4. Современные средства противодействия экономическому шпионажу<br>5. Современные криптографические системы<br>6. Криптоанализ, современное состояние<br>7. Правовые основы защиты информации<br>8. Технические аспекты обеспечения защиты информации. Современное состояние<br>9. Атаки на систему безопасности и современные методы защиты.<br>10. Современные пути решения проблемы информационной безопасности РФ |
| Информация как объект защиты. Государственная политика информационной безопасности. Концепция комплексного обеспечения защиты информации. | 11. Классификация информации. Виды данных и носителей.<br>12. Ценность информации. Цена информации.<br>13. Количество и качество информации.<br>14. Виды защищаемой информации.<br>15. Демаскирующие признаки объектов защиты.<br>16. Классификация источников и носителей информации.<br>17. мероприятия по управлению доступом к информации.<br>18. Функциональные источники сигналов. Опасный сигнал.<br>19. Основные средства и системы, содержащие потенциальные источники опасных сигналов. |

| | |
|---|---|
| | 20. Вспомогательные средства и системы, содержащие потенциальные источники опасных сигналов.<br>21. Виды паразитных связей и наводок, характерные для любых радиоэлектронных средств и проводов, соединяющих их кабелей.<br>22. Виды угроз безопасности информации.<br>23. Основные принципы добывания информации.<br>24. Процедура идентификации, как основа процесса обнаружения объекта.<br>25. Методы синтеза информации.<br>26. Методы несанкционированного доступа к информации.<br>27. Основными способами привлечения сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.<br>28. Способы наблюдения с использованием технических средств. |

**Задания для тестирования по дисциплине для оценки сформированности компетенций (min 20, max 50 + ссылку на ЭИОС с тестами)**

Программа, которая может размножаться, присоединяя свой код к другой программе, называется
Выберите один ответ.
a. Компилятор
b. Интернет-черви
c. Вирус

2. Величиной (размером) ущерба (вреда), ожидаемого в результате несанкционированного доступа к информации или нарушения доступности информационной системы, называется
Выберите один ответ.
a. Воздействием (влиянием)
b. Потерей
c. Силой

3. Код, способный самостоятельно, то есть без внедрения в другие программы, вызвать распространение своих копий по информационной системе и их выполнение, называется
Выберите один ответ.
a. Троянской программой
b. Червем
c. Вирусом

4. Уровень риска, который считается доступным для достижения желаемого результата, называется
Выберите один ответ.
a. Устойчивостью
b. Терпимостью по отношению к риску
c. Независимостью

5. Компьютер с одним процессором в каждый конкретный момент времени может выполнять команд
Выберите один ответ.
a. Две
b. Одну
c. Сколько зададут

6. Алгоритмы реального времени, заранее назначающие каждому процессу фиксированный приоритет, после чего выполняющие приоритетное планирование с переключениями, называются:
Выберите один ответ.

a. Статическими алгоритмами
b. Алгоритмы RMS
c. Динамическими алгоритмами

7. Системные файлы, обеспечивающие поддержку структур файловой системы, называются:
Выберите один ответ.
a. Каталоги
b. Символьные файлы
c. Регулярные файлы

8. Коды, обладающие способностью к распространению (возможно, с изменениями) путем внедрения в другие программы, называются
Выберите один ответ.
a. Вирусами
b. Руткитами
c. Червями

9. Требованием к информационной системе, являющимся следствием действующего законодательства, миссии и потребностей организации, называется:
Выберите один ответ.
a. Правилами безопасности
b. Требованием безопасности
c. Мерами безопасности

10. Процессом идентификации рисков применительно к безопасности информационной системы, определения вероятности их осуществления и потенциального воздействия, а также дополнительный контрмер, ослабляющий (уменьшающий) это воздействие, называется:
Выберите один ответ.
a. Управление риском
b. Предупреждением рисков
c. Анализом рисков

11. Компьютерная система, в которой два или более центральных процессоров делят полный доступ к общей оперативной памяти, называется
Выберите один ответ.
a. Мультипроцессоры типа «хозяин-подчиненный»
b. Симметричный мультипроцессор
c. Мультипроцессор с общей памятью

12. В число направлений физической защиты не входят:
физическая защита пользователей защита поддерживающей инфраструктуры
защита от перехвата данных

13.Криптография необходима для реализации следующих сервисов безопасности:
шифрование
туннелирование
разграничение доступа

14.В число целей политики безопасности верхнего уровня не входит:
решение сформировать или пересмотреть комплексную программу безопасности
обеспечение базы для соблюдения законов и правил
+обеспечение конфиденциальности почтовых сообщений

15.В число целей программы безопасности верхнего уровня входят:
управление рисками
определение ответственных за информационные сервисы
определение мер наказания за нарушения политики безопасности

16.В рамках программы безопасности нижнего уровня не осуществляется:
стратегическое планирование
повседневное администрирование
отслеживание слабых мест защиты

17.Политика безопасности строится на основе:
общих представлений об ИС организации
изучения политик родственных организаций
анализа рисков

18.В число целей политики безопасности верхнего уровня входят:
формулировка административных решений по важнейшим аспектам реализации
выбор методов аутентификации пользователей
обеспечение базы для соблюдения законов и правил +

19.В число целей программы безопасности верхнего уровня входят:
составление карты информационной системы
координация деятельности в области информационной безопасности
пополнение и распределение ресурсов

20.При анализе стоимости защитных мер не следует учитывать:
расходы на закупку оборудования
расходы на закупку программ
расходы на обучение персонала
расходы на премии персонала

**Практические задачи (min 20, max 50 + ссылку на ЭИОС с электронным изданием, если имеется)**

| Раздел дисциплины | Задачи |
|---|---|
| Основные понятия теории защиты информациии. Задачи защиты информации. | 1. Работа в одноранговой сети Windows<br>2. Основные нормативные руководящие документы информационной безопасности. Справочно-правовая система «Консультант Плюс»<br>3. Основные нормативные руководящие документы информационной безопасности. Справочно-правовая система «ГАРАНТ-Максимум<br>4. Стандарты информационного обмена<br>5. Работа с антивирусными программами<br>6. Программная реализация криптографических алгоритмов (Симметричные криптосистемы- шифр перестановки)<br>7. Программная реализация криптографических алгоритмов (алгоритмы двойных перестановок)<br>8. Программная реализация криптографических алгоритмов(Шифры простой замены)<br>9. Программная реализация криптографических алгоритмов(Шифры сложной замены) |
| Информация как объект защиты. Государственная политика информационной безопасности. Концепция комплексного | 10. Асимметричные криптосистемы.<br>11. Механизмы контроля целостности данных создать ЭЦП шифрованием профиля сообщения закрытым ключом<br>12. Механизмы контроля целостности данных создание профиля дешифрованием ЭЦП открытым ключом отправителя<br>13. Защита документов MS Office<br>14. Проект «Подготовка документов для разработки проекта политики и программы информационной безопасности предприятия» |

| | |
|---|---|
| обеспечения защиты информации. | 15. Задание 1 «Классификация угроз»<br>16. Задание 2 «Нормативно-методическое обеспечение СУИБ».<br>17. Задание 3 «Требования к кандидату на должность начальника службы безопасности коммерческой фирмы»<br>18. Задание 4 «Управление инцидентами ИБ» |

### 6.5. Оценочные материалы для промежуточной аттестации

**Фонд вопросов для проведения промежуточного контроля в форме экзамена**

| Раздел дисциплины | Вопросы |
|---|---|
| Основные понятия теории защиты информациии. Задачи защиты информации. | 1.Что такое информационная безопасность?<br>2. Какие предпосылки и цели обеспечения информационной безопасности?<br>3. В чем заключаются национальные интересы РФ в информационной сфере?<br>4. Что включает в себя информационная борьба?<br>5. Какие пути решения проблем информационной безопасности РФ существуют?<br>6. Каковы общие принципы обеспечения защиты информации?<br>7. Какие имеются виды угроз информационной безопасности предприятия (организации)?<br>8. Какие источники наиболее распространенных угроз информационной безопасности существуют?<br>9. Какие виды сетевых атак имеются?<br>10.Какими способами снизить угрозу сниффинга пакетов?<br>11.Какие меры по устранению угрозы IP -спуфинга существуют?<br>12.Что включает борьба с атаками на уровне приложений?<br>13.Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей?<br>14.В чем заключается распределенное хранение файлов?<br>15.Что включают в себя требования по обеспечению комплексной системы информационной безопасности?<br>16.Какие уровни информационной защиты существуют, их основные составляющие?<br>17.В чем заключаются задачи криптографии?<br>18.Зачем нужны ключи?<br>19.Какая схема шифрования называется многоалфавитной подстановкой?<br>20.Какие системы шифрования вы знаете?<br>21.Что включает в себя защита информации от несанкционированного доступа?<br>22.В чем заключаются достоинства и недостатки программноаппаратных средств защиты информации?<br>23.Какие виды механизмов защиты могут быть реализованы для обеспечения идентификации и аутентификации пользователей?<br>24.Какие задачи выполняет подсистема управления доступом?<br>25.Какие требования предъявляются к подсистеме протоколирования аудита?<br>26.Какие виды механизмов защиты могут быть реализованы для обеспечения конфиденциальности данных и сообщений?<br>27.В чем заключается контроль участников взаимодействия?<br>28.Какие функции выполняет служба регистрации и наблюдения?<br>29.Что такое информационно-опасные сигналы, их основные параметры? |

| | |
|---|---|
| | 30.Какие требования необходимо выполнять при экранировании помещений, предназначенных для размещения вычислительной техники?<br>31.Какой процесс называется аутентификацией пользователя?<br>32.Какие схемы аутентификации вы знаете?<br>33.Что такое смарт-карты?<br>34.Какие требования предъявляются к современным криптографическим системам защиты информации?<br>35.Что такое симметричная криптосистема?<br>36.Какие виды симметричных криптосистем существуют?<br>37.Что такое асимметричная криптосистема?<br>38.Что понимается под односторонней функцией?<br>39.Как классифицируются криптографические алгоритмы по стойкости?<br>40.В чем заключается анализ надежности криптосистем?<br>41.Что такое дифференциальный криптоанализ?<br>42.В чем сущность криптоанализа со связанными ключами?<br>43.В чем сущность линейного криптоанализа?<br>44.Какие атаки изнутри вы знаете? |
| Информация как объект защиты. Государственная политика информационной безопасности. Концепция комплексного обеспечения защиты информации. | 45.Какая программа называется логической бомбой?<br>46.Какими способами можно проверить систему безопасности?<br>47.Что является основными характеристиками технических средств защиты информации?<br>48.Какие требования предъявляются к автоматизированным системам защиты третьей группы?<br>49.Какие требования предъявляются к автоматизированным системам защиты второй группы?<br>50.Какие требования предъявляются к автоматизированным системам защиты первой группы?<br>51.Какие классы защиты информации от несанкционированного доступа для средств вычислительной техники имеются? От чего зависит выбор класса защищенности?<br>52.Какие требования предъявляются к межсетевым экранам?<br>53.Какие имеются показатели защищенности межсетевых экранов?<br>54.Какие атаки системы снаружи вы знаете?<br>55.Какая программа называется вирусом?<br>56.Какая атака называется атакой отказа в обслуживании?<br>57.Какие виды вирусов вы знаете?<br>58.Какие вирусы называются паразитическими?<br>59.Как распространяются вирусы?<br>60.Какие методы обнаружения вирусов вы знаете?<br>61.Какая программа называется монитором обращения?<br>62.Что представляет собой домен?<br>63.Как осуществляется защита при помощи ACL -списков?<br>64.Какой список называется перечнем возможностей?<br>65.Какие способы защиты перечней возможностей вы знаете?<br>66.Из чего состоит высоконадежная вычислительная база (TCB)?<br>67.Какие модели многоуровневой защиты вы знаете?<br>68.В чем заключается организация работ по защите от несанкционированного доступа интегрированной информационной системы управления предприятием?<br>69.Какие характеристики положены в основу системы классификации информационных систем управления предприятием?<br>70.Какие задачи решает система компьютерной безопасности?<br>71.Какие пути защиты информации в локальной сети существуют?<br>72.Какие задачи решают технические средства противодействия экономическому шпионажу? |

| | |
|---|---|
| | 73.Какой порядок организации системы видеонаблюдения?<br>74.Что включает в себя защита информационных систем с помощью планирования?<br>75.Какие условия работы оцениваются при планировании?<br>76.Из каких этапов состоят работы по обеспечению информационной безопасности предприятия?<br>77.Что такое мобильные программы?<br>78.Что такое концепция потоков?<br>79.Что представляет собой метод «песочниц»?<br>80.Что такое интерпретация?<br>81.Что такое программы с подписями?<br>82.Что представляет собой безопасность в системе Java ?<br>83.Назовите несколько примеров политик безопасности пакета JDK 1.2?<br>84.Какие международные документы регламентируют деятельность по обеспечению защиты информации?<br>85.Что понимают под политикой информационной безопасности?<br>86.Что включает в себя политика информационной безопасности РФ?<br>87.Какие нормативные документы РФ определяют концепцию защиты информации? |

**6.6. Шкалы и критерии оценивания по формам текущего контроля и промежуточной аттестации**

**Шкала и критерии оценивания**

| Оценка | Критерии оценивания для мероприятий контроля с применением 4-х балльной системы |
|---|---|
| **«отлично»** | Повышенный ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-4.3 |
| **«хорошо»** | Стандартный ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-4.3 |
| **«удовлетворительно»** | Пороговый ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК- 3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-4.3 |
| **«неудовлетворительно»** | Результаты обучения не сформированы на пороговом уровне |