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

Институт Институт национальной и мировой экономики

Кафедра Прикладной информатики

УТВЕРЖДЕНО
Ученым советом Университета
(протокол № 10 от 22 мая 2025 г.)

РАБОЧАЯ ПРОГРАММА

Наименование дисциплины Б1.В.ДЭ.04.02 Техническая защита информации

Основная профессиональная образовательная программа 01.03.05 Статистика программа Информационные системы на финансовых рынках

Квалификация (степень) выпускника бакалавр

Самара 2025

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 Техническая защита информации входит в часть, формируемая участниками образовательных отношений (дисциплина по выбору) блока Б1.Дисциплины (модули)

Последующие дисциплины по связям компетенций: Анализ и оценка финансовых рисков проекта, Проектный практикум, Портфельное инвестирование, Оптимизация инвестиционного портфеля

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

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

Профессиональные компетенции (ПК):

ПК-5 - Способен осуществлять административное сопровождение проектов в области инновационных финансовых технологий

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
ПК-5	ПК-5.1: Знать:	ПК-5.2: Уметь:	ПК-5.3: Владеть (иметь навыки):
	ключевые положения процесса администрирования сопровождения проектов в области инновационных финансовых технологий	управлять процессом реализации проектов в области инновационных финансовых технологий	навыками административной работы и сопровождения проектов в области инновационных финансовых технологий

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:	36.15/1
Занятия лекционного типа	18/0.5
Занятия семинарского типа	18/0.5
Индивидуальная контактная работа (ИКР)	0.15/0
Самостоятельная работа:	17.85/0.5
Промежуточная аттестация	18/0.5
Вид промежуточной аттестации: Зачет	 Зач
Общая трудоемкость (объем части образовательной программы): Часы Зачетные единицы	72 2

4. Содержание дисциплины

4.1. Разделы, темы дисциплины и виды занятий:

Тематический план дисциплины Техническая 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	ИКР	ГКР		
			Практич. занятия				
1.	Организация и проведение работ по технической защите информации	8	8	0,075		12	ПК-5.1, ПК-5.2, ПК -5.3
2.	Защита информации от несанкционированного доступа	10	10	0,075		5.85	ПК-5.1, ПК-5.2, ПК -5.3
	Контроль	18					
	Итого	**18**	**18**	**0.15**		**17.85**	

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.	Организация и проведение работ по технической защите информации	лекция	Защита информации и информационных ресурсов, объекты защиты
		лекция	Организационно-правовые основы защиты информации
		лекция	Угрозы безопасности информации
		лекция	Формирование требований по защите информации и создание системы защиты информации
2.	Защита информации от несанкционированного доступа	лекция	Организационно-технические основы выполнения мероприятий по защите информации от несанкционированного доступа
		лекция	Меры и средства защиты информации от несанкционированного доступа
		лекция	Методы и средства контроля защищённости информации от несанкционированного доступа
		лекция	Сертификация средств по защите информации от несанкционированного доступа
		лекция	Администрирование системы защиты информации от несанкционированного доступа

*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.	Организация и проведение работ по технической защите информации	практическое занятие	Введение в информационную безопасность. Стандарты и организации, работающие в области информационной безопасности
		практическое занятие	Методики проведения работ по защите информации
		практическое занятие	Определения видов и типов угроз и способы защиты от них
		практическое занятие	Построение системы безопасности организации
2.	Защита информации от несанкционированного доступа	практическое занятие	Руководящие документы от несанкционированного доступа
		практическое занятие	Выбор мер и средств защиты от несанкционированного доступа
		практическое занятие	Применение методов и средств защиты информации от несанкционированного доступа
		практическое занятие	Программно-аппаратные средства защиты информации
		практическое занятие	Управление системой защиты информации от несанкционированного доступа

** 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.	Организация и проведение работ по технической защите информации	- подготовка доклада - подготовка электронной презентации - тестирование
2.	Защита информации от несанкционированного доступа	- подготовка доклада - подготовка электронной презентации - 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. Внуков, А. А. Защита информации : учебник для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 161 с. — (Высшее образование). — ISBN 978-

5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561313
2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2025. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/562070

Дополнительная литература

1. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2025. — 349 с. — (Высшее образование). — ISBN 978-5-534-19762-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561077
2. Внуков, А. А. Защита информации в банковских системах : учебник для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2025. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561314

Литература для самостоятельного изучения

Казарин, О. В. Надежность и безопасность программного обеспечения : учебник для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2025. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/563862

Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2025. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560804

Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2025. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561432

Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567672

5.2. Перечень лицензионного программного обеспечения

1. Astra Linux Special Edition «Смоленск», «Орел»; РедОС ; ОС "Альт Рабочая станция" 10; ОС "Альт Образование" 10
2. МойОфис Стандартный 2, МойОфис Образование, Р7-Офис Профессиональный, МойОфис Стандартный 3, МойОфис Профессиональный 3

5.3 Современные профессиональные базы данных, к которым обеспечивается доступ обучающихся

1. Профессиональная база данных «Информационные системы Министерства экономического развития Российской Федерации в сети Интернет» (Портал «Официальная Россия» - http://www.gov.ru/)
2. Государственная система правовой информации «Официальный интернет-портал правовой информации» (http://pravo.gov.ru/)
3. Профессиональная база данных «Финансово-экономические показатели Российской Федерации» (Официальный сайт Министерства финансов РФ - https://www.minfin.ru/ru/)

4. Профессиональная база данных «Официальная статистика» (Официальный сайт Федеральной службы государственной статистики - http://www.gks.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 Мультимедийный проектор Доска Экран
Учебные аудитории для проведения практических занятий (занятий семинарского типа)	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения оборудования

6. Фонд оценочных средств по дисциплине Техническая защита информации:

6.1. Контрольные мероприятия по дисциплине

Вид контроля	**Форма контроля**	**Отметить нужное знаком « + »**
Текущий контроль	Оценка докладов	+
	Устный/письменный опрос	–
	Тестирование	+
	Практические задачи	+

Промежуточный контроль	Зачет	+

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-5 - Способен осуществлять административное сопровождение проектов в области инновационных финансовых технологий

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	ПК-5.1 Знать	ПК-5.2 Уметь	ПК-5.3 Владеть
	ключевые положения процесса администрирования сопровождения проектов в области инновационных финансовых технологий	управлять процессом реализации проектов в области инновационных финансовых технологий	навыками административной работы и сопровождения проектов в области инновационных финансовых технологий
Пороговый	Ключевые положения и этапы жизненного цикла проекта. Основы документооборота и административной отчетности в проектной деятельности.	Выполнять административные функции: вести протоколы встреч, составлять отчеты о статусе проекта, работать с проектной документацией.	Навыками делопроизводства и организации документооборота проекта.
Стандартный (в дополнение к пороговому)	Основные методологии управления проектами (Agile, Scrum, Waterfall). Принципы управления ресурсами, рисками и коммуникациями в проекте.	Управлять отдельными процессами проекта: планировать задачи, отслеживать исполнение, идентифицировать и документировать риски. Организовывать коммуникацию между участниками рабочей группы.	Навыками использования ПО для управления проектами (Jira, Asana, Trello). Навыками оперативного административного сопровождения и контроля выполнения проектных задач.

Повышенный (в дополнение к пороговому и стандартному)	Передовые практики управления проектами (PMBOK, PRINCE2). Особенности управления IT- и FinTech-проектами, включая работу с удаленными командами.	Осуществлять полное административное сопровождение проекта: управлять бюджетом, сроками, качеством и содержанием проекта. Адаптировать процессы управления под специфические требования FinTech-проекта и команды.	Навыками полноценного project-администрирования на всех этапах жизненного цикла FinTech-проекта. Навыками антикризисного управления и разрешения сложных ситуаций в проекте.

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.	Организация и проведение работ по технической защите информации	ПК-5.1, ПК-5.2, ПК-5.3	Оценка докладов Устный/письменный опрос Тестирование	Зачет
2.	Защита информации от несанкционированного доступа	ПК-5.1, ПК-5.2, ПК-5.3	Оценка докладов Тестирование Практические задачи	Зачет

6.4. Оценочные материалы

Примерная тематика докладов

Раздел дисциплины	Темы
Организация и проведение работ по технической защите информации	1. Методы и способы защиты информации в современных информационных системах: обзор актуальных технологий и подходов к технической защите данных 2. Нормативно-правовая база в области технической защиты информации: законодательство, стандарты (ФСТЭК, ФСБ, ГОСТ), международные требования 3. Угрозы информационной безопасности: классификация и методы противодействия (внешние и внутренние угрозы, социальная инженерия, кибератаки) 4. Защита конфиденциальной информации в корпоративных сетях: DLP-системы, шифрование, контроль доступа 5. Криптографические методы защиты информации: алгоритмы шифрования, электронные подписи, криптографические протоколы

	6. Обеспечение безопасности беспроводных сетей: Wi-Fi, Bluetooth, IoT-устройства, методы взлома и защита 7. Применение искусственного интеллекта в технической защите информации: AI для обнаружения аномалий, анализа угроз и автоматизации защиты 8. Антивирусная защита: современные технологии и тренды: эвристический анализ, песочницы, поведенческие сигнатуры 9. Облачные технологии и их безопасность: риски SaaS, IaaS, PaaS, методы защиты облачных данных 10. Методы защиты от атак типа "человек посередине" (MITM): перехват трафика, способы предотвращения, использование VPN и TLS 11. Защита персональных данных в соответствии с ФЗ-152 (требования, меры защиты, аудит и сертификация) 12. Роль биометрии в системах аутентификации и защиты информации (отпечатки, распознавание лиц, голосовая аутентификация) 13. Пентестинг (тестирование на проникновение) как метод оценки защищённости 14. Обеспечение безопасности промышленных систем (АСУ ТП, SCADA, IoT) 15. Инциденты информационной безопасности: расследование и реагирование: формирование CSIRT, SOC, анализ цифровых улик, Digital Forensics
Защита информации от несанкционированного доступа	16. Основные угрозы и виды несанкционированного доступа к информации 17. Методы аутентификации и авторизации для обеспечения информационной безопасности 18. Шифрование данных как средство защиты информации 19. Роль фаерволов и систем обнаружения вторжений в защите информации 20. Политики безопасности и их внедрение в корпоративных информационных системах 21. Обучение сотрудников и культура безопасности как важные компоненты защиты информации Технологии защиты персональных данных в соответствии с законами и стандартами 22. Обзор современных методов защиты информации: блокчейн, искусственный интеллект и их роль 23. Практические кейсы: анализ инцидентов нарушения безопасности и методы их предотвращения

Задания для тестирования/ практические задачи по дисциплине для оценки сформированности компетенции: ПК-5 - Способен осуществлять административное сопровождение проектов в области инновационных финансовых технологий

<table>
<tr><th>№ п/п</th><th>Задание</th><th>Ключ к заданию / Эталонный ответ</th></tr>
<tr><td>1.</td><td>При административном сопровождении проектов обеспечивающим информационную безопасность используют следующие правовые методы:
1. Разработка аппаратных средств обеспечения правовых данных
2. Разработка и установка во всех компьютерных правовых сетях журналов учета действий
3. Разработка и конкретизация правовых нормативных актов обеспечения безопасности</td><td>3</td></tr>
<tr><td>2.</td><td>Основными источниками угроз в области инновационных финансовых технологий информационной безопасности являются все указанное в списке:
1. Хищение жестких дисков, подключение к сети, инсайдерство
2. Перехват данных, хищение данных, изменение архитектуры системы
3. Хищение данных, подкуп системных администраторов, нарушение регламента работы</td><td>2</td></tr>
<tr><td>3.</td><td>Виды информационной безопасности при административном сопровождении проектов:
1. Персональная, корпоративная, государственная
2. Клиентская, серверная, сетевая
3. Локальная, глобальная, смешанная</td><td>1</td></tr>
<tr><td>4.</td><td>Цели информационной безопасности в области инновационных финансовых технологий – своевременное обнаружение, предупреждение:
1. несанкционированного доступа, воздействия в сети
2. инсайдерства в организации
3. чрезвычайных ситуаций</td><td>1</td></tr>
<tr><td>5.</td><td>При административном сопровождении проектов основными объектами информационной безопасности являются:
1. Компьютерные сети, базы данных
2. Информационные системы, психологическое состояние пользователей
3. Бизнес-ориентированные, коммерческие системы</td><td>1</td></tr>
<tr><td>6.</td><td>В области инновационных финансовых технологий основными рисками информационной безопасности являются:
1. Искажение, уменьшение объема, перекодировка информации
2. Техническое вмешательство, выведение из строя оборудования сети
3. Потеря, искажение, утечка информации</td><td>3</td></tr>
<tr><td>7.</td><td>К основным принципам обеспечения информационной безопасности при административном сопровождении проектов относятся:
1. Экономической эффективности системы безопасности
2. Многоплатформенной реализации системы
3. Усиления защищенности всех звеньев системы</td><td>1</td></tr>
<tr><td>8.</td><td>Установите соответствие между криптопримитивом и его назначением при административном сопровождении проектов
<table>
<tr><th>Криптопримитив</th><th>Назначение</th></tr>
<tr><td>1. Криптографическая хеш-функция</td><td>А. Защита от радужных таблиц при хранении хешей</td></tr>
<tr><td>2. Цифровая подпись</td><td>Б. Конфиденциальность данных</td></tr>
<tr><td>3. Симметричное шифрование</td><td>В. Проверка целостности сообщений</td></tr>
</table></td><td>
<table>
<tr><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td>В</td><td>Г</td><td>Б</td><td>А</td></tr>
</table>
</td></tr>
</table>

4. Случайная соль	Г. Аутентификация и неотрекаемость отправителя	

9. При административном сопровождении проектов, соотнесите основные методы получения паролей:

Методы	**Назначение**
1. Метод тотального перебора	А. Для перебора используется словарь наиболее вероятных ключей
2. Словарная атака	Б. Двумя возможностями выяснения пароля являются: несанкционированный доступ к носителю, содержащему пароли, либо использование уязвимостей
3. Получение паролей из самой системы на основе программной и аппаратной реализации конкретной системы	В. Проверяются все ключи последовательно, один за другим
4. Проверка паролей, устанавливаемых в системах по умолчанию	Г. Пароль, установленный фирмой-разработчиком по умолчанию, остается основным паролем в системе

1	2	3	4
В	А	Б	Г

10. В области инновационных финансовых технологий соотнесите принципы информационной безопасности, определенные Гостехкомиссией

Принцип	**Действие**
1. Принцип системности	А. Правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми
2. Принцип комплексности	Б. Непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС
3. Принцип комплексности	В. Предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов
4. Гибкость системы защиты	Г. Предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов

1	2	3	4
Г	В	Б	А

11. При административном сопровождении проектов, соотнесите основные понятия в области информационной безопасности:

Понятие	Действие
1. Атака	А. Некоторое неудачное свойство системы, которое делает возможным возникновение и реализацию угрозы
2. Уязвимость АС	Б. Система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности
3. Угроза безопасности АС	В. Возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности
4. Защищенная система	Г. Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы

1	2	3	4
Г	А	В	Б

12. Соотнесите функции, выполняемые техническими средствами защиты в области инновационных финансовых технологий:

Функции	Защита
1. Внешняя защита	А. Защита от воздействия дестабилизирующих факторов, проявляющихся за пределами основных средств АСОД
2. Опознавание	Б. Специфическая группа средств, предназначенных для опознавания людей по различным индивидуальным харак- теристикам
3. Внутренняя защита	В. Защита от воздействия дестабилизирующих факторов, проявляющихся непосредственно в средствах обработки информации
4. Сканирование	Г. Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы

1	2	3	4
Б	В	А	Г

13. В области инновационных финансовых технологий в информационной безопасности соотнесите степени сложности устройств:

Степени сложности устройств	Устройства
1. Простые устройства	А. Комбинированные агрегаты, состоящие из некоторого количества простых устройств, способные к осуществлению сложных процедур защиты;

1	2	3	4
Б	В	А	Г

	2. Системы	Б. Несложные приборы и приспособления, выполняющие отдельные процедуры защиты;	
	3. Сложные устройства	В. Законченные технические комплексы, способные осуществлять некоторую комбинированную процедуру защиты, имеющую самостоятельное значение;	
	4. Подсистемы	Г. Встроенные в единую систему и могут осуществлять взаимодействие друг с другом	
14.	В административном сопровождении проектов в области защиты информации соотнесите классификацию угроз по ряду признаков:		
	Классификация угроз	**Признаки**	
	1. По природе возникновения	А. Пассивные и активные	
	2. По непосредственному источнику	Б. Направленные на использование прямого стандартного пути доступа к ресурсам и направленные на использование скрытого нестандартного доступа к ресурсам АС	
	3. По степени воздействия на АС	В. Естественные или искусственные	
	4. По способу доступа к ресурсам АС	Г. Природная среда, человек, санкционированные программные средства и несанкционированные программные средства	

1	2	3	4
А	Б	В	Г

15.	При административном сопровождении проектов, сотрудник открыл вредоносное письмо, перешел по ссылке и ввел свои учетные данные на поддельном сайте, который имитировал внутренний портал компании. В результате были скомпрометированы логины и пароли нескольких сотрудников. Какие меры необходимо предпринять для устранения инцидента и предотвращения подобных атак в будущем?	1. Немедленная изоляция: отключить скомпрометированные учетные записи от сети. 2. Анализ инцидента: провести расследование, чтобы определить, какие именно данные были украдены и какие системы затронуты. 3. Усиление безопасности: сбросить пароли для всех сотрудников, провести тренинг по кибербезопасности с акцентом на социальную инженерию. 4. Мониторинг: включить дополнительные средства мониторинга для выявления подозрительной активности.
16.	В области инновационных финансовых технологий на предприятии произошла авария на трубопроводе, и вода начала заливать помещение серверной. Какие шаги нужно предпринять для минимизации ущерба и восстановления работы?	1. Аварийное отключение: немедленно отключить электропитание серверов, если это безопасно. 2. Эвакуация оборудования: при возможности, эвакуировать оборудование в безопасное место.

		3. Включение резервного питания: активировать резервные источники питания и системы бесперебойного питания (ИБП) для сохранения работы критически важных систем. 4. Аварийное восстановление: запустить процесс восстановления из резервных копий данных.
17.	При административном сопровождении проектов в области защиты информации один из сотрудников оставил свой рабочий компьютер с открытым доступом в переговорной комнате, а другой сотрудник, не имея на то права, получил доступ к конфиденциальным файлам проекта. Как можно было предотвратить эту ситуацию и что предпринять сейчас?	1. Принцип минимальных привилегий: применять принцип минимальных привилегий, когда доступ к информации предоставляется только тем, кому это необходимо для работы. 2. Политика паролей и блокировка сеансов: ввести обязательную блокировку рабочей станции при любом отходе от нее, а также требование смены паролей. 3. Аудит доступа: провести аудит прав доступа к конфиденциальным данным. 4. Обучение сотрудников: провести обучение сотрудников по основам ИБ, обращая внимание на важность защиты своих учетных данных.
18.	При административном сопровождении проектов в области защиты информации сотрудник МВД при проведении служебных совещаний, на которых обсуждались сведения, составляющие государственную тайну (далее - ССГТ), брал с собой смартфон. Им неоднократно фотографировались ССГТ, чтобы затем использовать эти сведения в служебной деятельности. Правомерно ли был им получен доступ к ССГТ? Соблюдал ли он правила ознакомления с ССГТ? Где он мог делать пометки со служебных совещаний?	Сотрудник в своей деятельности нарушил внутренний приказ министра своего ведомства а также закон о ГТ, который предписывает при обработке ССГТ использовать только учтённые носители, которые хранятся и учитываются особым образом. Его действия имели предпосылку к ознакомлению с ССГТ неограниченного круга лиц. В ходе очередного совещания, его действия были замечены начальником подразделения и было начато служебное разбирательство по данному факту. В результате этого разбирательства, при осмотре устройства и дачи показаний было выяснено, что эти фотографии пересылались сотрудником в мессенджерах коллегам по работе и было обсуждение служебных вопросов.
19.	При административном сопровождении проектов в области защиты информации один из студентов решил использовать компьютер из компьютерного класса университета для оформления контрольных и курсовых работ. Без разрешения деканата факультета он проник в класс и стал работать на компьютере. Из-за крайне поверхностных знаний и навыков работы на компьютере произошли сбои в работе машины, что привело в дальнейшем к отключению модема - одного из элементов компьютерной системы.	Родовым объектом данного преступления являются общественная безопасность и общественный порядок; видовым – отношения в сфере компьютерной безопасности. Непосредственный объект – это отношения, обеспечивающие правила эксплуатации хранения, обработки, передачи компьютерной информации и информационно-телекоммуникационных сетей. Объективная сторона преступления сконструирована в качестве материального состава. Обязательные условия наступления уголовной ответственности – причинение крупного ущерба. В деянии

		студента усматриваются отдельные признаки объективной стороны деяния, в частности, нарушения правил эксплуатации информационно-телекоммуникационных сетей.
20.	При административном сопровождении проектов в области защиты информации на одном из предприятий возникла необходимость отправить документы в Министерство Обороны РФ (далее МО), подписанные электронной подписью одного из руководителей. МО прислали инструкцию, ЭЦП для подписания есть у директора и его заместителя (Рутокен ЭЦП 2.0). При подписании документов ЭЦП директора, КриптоАРМ выдал ошибку: «Нет полного доверия к сертификату подписи», а после подписания документов другой подписью, при загрузке их на ресурс МО, появляется ошибка, что сертификат недействителен. При этом заведомо известно, что обе подписи действительны. Получатель посоветовал подписать документы на другом компьютере, но при установке носителя КриптоАРМ не видит сертификатов на носителях, при этом всплывает окно «Установка заблокирована групповой политикой». Почему может появиться такая ошибка о доверии к сертификату? Можно ли проверить действительность сертификатов и как, с помощью какой программы, можно это сделать. Как решить проблему с определением сертификатов на другом компьютере?	Для решения первой проблемы, необходимо загрузить список отозванных сертификатов и импортировать его в Крипто АРМ. Далее, проверить любые свойства сертификата (срок действия, информация о выданной организации и т.п.) можно с помощью панели управления Рутокен, открыть сертификат и перейти во вкладку «Свойства» При установке носителя в новый компьютер необходимы драйвера (в данном случае Рутокен), скорее всего на данном компьютере они отсутствуют. Сообщение «Установка заблокирована групповой политикой» может говорить о том, что USB порты отключены групповыми политиками предприятия, поэтому необходимо обратиться к системному администратору, чтобы он внес изменения в групповую политику.
21.	В области инновационных финансовых технологий молодой человек по имени Андрей решил закупить себе скины (уникальная покраска оружия) для игры Counter-Strike: Global Offensive на сайте, где они продаются по меньшей цене, чем на торговой площадке Steam. Час он пытался зайти на этот сайт, авторизовываясь с помощью данных аккаунта Steam. Когда ему надоело, он решил всё же купить скины на торговой площадке Steam и понял, что не может зайти в свой аккаунт. Посмотрев информацию об аккаунте через браузер, он осознал, что тот сайт был фишинговым и его данные аккаунта украли. Как можно было обезопасить свой Steam аккаунт, чтобы его не могли взломать? Что делать теперь, после того, как данные профиля украдены?	1. Установить антивирусную программу. 2. Использовать максимально надёжный и защищённый почтовый сервис. 3. Активировать Steam Guard. 4. Придумать оригинальный и сложный пароль. 5. Никому и никогда не разглашать свой логин и пароль. 6. Сделать привязку аккаунта к номеру мобильного телефона. 7. Настроить приватность профиля под себя.

6.5. Комплект оценочных средств для промежуточной аттестации

Примерные вопросы к зачету

Контролируемые компетенции – ПК-5 - Способен осуществлять административное сопровождение проектов в области инновационных финансовых технологий

№ п/п	Задание	Ключ к заданию / Эталонный ответ
1.	В рамках осуществления административного сопровождения проектов в области защиты информации дайте определение информационной безопасности	Это состояние защищённости информации, при котором обеспечены её конфиденциальность, целостность и доступность
2.	Какую роль играют криптографические хеш-функции в области инновационных финансовых технологий?	Криптографическая хеш-функция отображает произвольные данные в фиксированный отпечаток, устойчивый к поиску прообразов и коллизий. В блокчейне хеш-значения связывают блоки: изменение байта в прошлом ведёт к изменению всех последующих хешей. Это свойство делает подмену истории обнаруживаемой без полного перерасчёта всеми участниками.
3.	В рамках административного сопровождения проектов что такое шифрование информации и его виды?	Шифрование информации — это процесс преобразования данных в нечитаемый вид (шифр-текст) с помощью специального алгоритма и ключа, чтобы защитить их от несанкционированного доступа и обеспечить конфиденциальность. Основные виды шифрования — симметричное, где используется один общий секретный ключ для

		шифрования и расшифровки, и асимметричное, где применяются два разных ключа: общедоступный (открытый) для шифрования и закрытый (секретный) для расшифровки
4.	В области инновационных финансовых технологий что такое стеганография?	Стеганогра́фия — способ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи (хранения). В отличие от криптографии, которая скрывает содержимое тайного сообщения, стеганография скрывает сам факт его существования. Как правило, сообщение будет выглядеть как что-либо иное, например, как изображение, статья, список покупок, письмо или судоку..
5.	Что такое несанкционированный доступ к информации в административном сопровождении проектов ?	Несанкционированный доступ — доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.
6.	Что такое техническая защита информации в рамках административного сопровождения проектов?	Техническая защита информации (ТЗИ) – это комплекс мероприятий, направленных на предотвращение утечки защищаемой информации по техническим каналам, на предотвращение несанкционированного доступа к ней, ее модификации, искажения, копирования, блокирования или уничтожения. ТЗИ является обязательной и неотъемлемой частью общей системы защиты информации на предприятии наряду с правовыми, организационными и другими мерами.
7.	В области инновационных финансовых технологий перечислите виды ТЗИ?	Программные средства защиты информации, аппаратные средства защиты информации, организационно-технические, инженерно-технические.
8.	Определение политики безопасности в сопровождении проектов?	Политика безопасности — это набор документированных правил, процедур и принципов, определяющих, как организация защищает свои информационные ресурсы и системы от угроз, обеспечивает их конфиденциальность, целостность и доступность.
9.	Зачем нужны в инновационных финансовых технологиях мульти-подписи?	Мульти-подписи и пороговые схемы авторизации требуют нескольких независимых подтверждений для выполнения критичных операций. Подход снижает риск, связанный с компрометацией одного ключа или ошибкой одного ответственного лица. Правило «k из n» обеспечивает проведение транзакций даже при недоступности части подписантов.
10.	Понятие хэш функции в финансовых технологиях?	Хеш-функция — это математический алгоритм, который преобразует данные любого размера в короткую строку символов фиксированной длины (хеш), уникальную для каждого набора входных данных. Она применяется в компьютерных науках и информационной безопасности для проверки целостности данных, безопасного хранения паролей, создания цифровых подписей и работы блокчейна.
11.	Перечислите 3 основных свойств защиты информации в области сопровождения проектов?	Конфиденциальность, целостность, доступность.
12.	Термин ”компьютерная сеть” в административном управлении	Компьютерная сеть — это совокупность взаимосвязанных компьютеров и других устройств, которые позволяют обмениваться информацией, совместно использовать ресурсы (например, принтеры, интернет-соединения) и выполнять вычисления.
13.	Дать определение компьютерного вируса в инновационных системах и технологиях?	Компьютерный вирус – это вид вредоносной программы, которая самостоятельно создает и распространяет свои копии, внедряясь в другие программы, файлы и системные области компьютера или сети. Его основная цель — самовоспроизведение и выполнение нежелательных действий, таких как повреждение или кража данных, нарушение работоспособности системы, блокировка доступа или кража информации.
14.	Что такое технический канал утечки информации при сопровождении проектов из чего состоит?	ТКУИ — это путь, по которому конфиденциальные данные несанкционированно передаются от источника к злоумышленнику через физическую среду при помощи технических средств. Он состоит из трех основных элементов: источника сигнала (объекта, излучающего или обрабатывающего информацию), физической среды (воздуха, кабелей, конструкций) и средства перехвата (приемника злоумышленника).
15.	Виды ТКУИ при управлении проектами?	Оптические; Радиоэлектронные; Акустические; Материально-вещественные.

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 2-х балльной системы
«зачтено»	ПК-5
«не зачтено»	Результаты обучения не сформированы на пороговом уровне