Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«Академия управления городской средой, градостроительства и печати»

УТВЕРЖДАЮ
Заместитель директора
по учебно-производственной работе
О.В. Фомичева
«25» декабря 2023 г.

КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ

по текущему контролю успеваемости
и промежуточной аттестации
по учебной дисциплине
ОП.01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

программы подготовки специалистов среднего звена

по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Санкт-Петербург
2023 г.

Комплект контрольно-оценочных средств по учебной дисциплине разработан на основе Федерального государственного образовательного стандарта по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Минобрнауки России от 09.12.2016 № 1553, в соответствии с рабочей программой учебной дисциплины ОП.01 Основы информационной безопасности.

Комплект контрольно-оценочных средств рассмотрен на заседании методического совета СПб ГБПОУ «АУГСГиП»

Протокол № 2 от «29» ноября 2023 г.

Комплект контрольно-оценочных средств одобрен на заседании цикловой комиссии общетехнических дисциплин и компьютерных технологий
Протокол № 4 от «21» ноября 2023 г.

Председатель цикловой комиссии: Караченцева М.С. _____

Разработчики: преподаватели СПб ГБПОУ «АУГСГиП»

С О Д Е Р Ж А Н И Е

1. Паспорт комплекта оценочных средств

В результате освоения учебной дисциплины «Основы информационной безопасности» обучающийся должен обладать следующими умениями, знаниями, которые формируют профессиональные и общие компетенции:

Знания:

— сущность и понятие информационной безопасности, характеристику ее составляющих;

— источники угроз информационной безопасности и меры по их предотвращению;

— жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;

— современные средства и способы обеспечения информационной безопасности.

Умения:

— классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;

— применять основные правила и документы системы сертификации Российской Федерации;

— классифицировать основные угрозы безопасности информации.

Общие компетенции:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Профессиональные компетенции:

ПК 1.6. Обеспечивать технику безопасности при проведении организационно-технических мероприятий.

ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах.

ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.

ПК 3.3. Проводить регламентные работы и фиксировать отказы средств защиты.

ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.

Формой **промежуточной аттестации** по учебной дисциплине является экзамен.

Текущий контроль освоения обучающимися программного материала учебной дисциплины проводится с целью объективной оценки качества освоения программы учебной дисциплины, а также стимулирования учебной работы обучающихся, мониторинга результатов образовательной деятельности, подготовки к промежуточной аттестации и обеспечения максимальной эффективности учебно-воспитательного процесса.

2. Результаты освоения учебной дисциплины, подлежащие проверке

2.1. В результате аттестации по учебной дисциплине осуществляется комплексная проверка следующих умений и знаний, а также динамика формирования общих компетенций:

Таблица 1

Контроль и оценка результатов освоения дисциплины

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Умения	
— классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; — применять основные правила и документы системы сертификации Российской Федерации; — классифицировать основные угрозы безопасности информации.	Оценка практических работ
Знания	
— сущность и понятие информационной безопасности, характеристику ее составляющих; — источники угроз информационной безопасности и меры по их предотвращению; — жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи; — современные средства и способы обеспечения информационной безопасности.	Устные зачеты Устные ответы на экзамене

3. Оценка освоения учебной дисциплины

3.1. Текущий контроль. Задания для текущей аттестации

Проводится преподавателем на учебных занятиях, согласно календарно-тематическому плану. Формы текущего контроля выбраны, исходя из методической целесообразности.

Таблица 2

Распределение контрольных точек по дисциплине

Дидактические единицы	**Проверяемые ОК, ПК, У, З**	**Формы контроля (наименование контрольной точки)**		
		Текущая аттестация		**Промежуточная аттестация**
Тема 1. Критическая информационная инфраструктура (КИИ) РФ	ОК 1, ОК 4, ОК 8, ПК 3.4., ПК 3.3., З2	Устный зачет по Теме 1		Устные ответы на экзамене
Тема 2. Сущность и понятие информационной безопасности (ИБ), характеристика составляющих ИБ	ОК 1, ОК 2, ОК, 4, ПК 3.4., У3, З1, З3	Практическая работа № 2 «Классификация угроз информационной безопасности»	Устный зачет по Темам 2-3	
Тема 3. Информация как объект защиты	ОК 1, ОК 2, ОК4, ОК 5, ПК 3.4, У1, У2, З4	Практическая работа № 4 «Классификация информации по видам тайн и степеням конфиденциальности»		
Тема 4. Меры по предотвращению угроз. Современные средства и способы обеспечения информационной безопасности	ОК1, ОК4, ОК 5, ОК 9, ПК 1.6., ПК3.1., ПК 3.2., ПК1.6, У1, У3, З4	Практическая работа № 5 «Работа с моделями доступа, определение степени конфиденциальности информации»	Устный зачет по Темам 4-5	
Тема 5. Защита от внутренних угроз. DLP-системы	ОК 1, ОК 4, ОК 5, ОК 9, ПК 3.1, ПК3.2, У3, З5	Практическая работа № 7 «Определение внутренних угроз информационной безопасности»		
Тема 6. Нарушитель ИБ	ОК 1, ОК 4, ОК 5, ПК.3.4., У3	Практическая работа № 8 «Определение характеристик нарушителя ИБ в зависимости от угрозы инфор-	Устный зачет по темам	

Дидактические единицы	Проверяемые ОК, ПК, У, З	Формы контроля (наименование контрольной точки)		
		Текущая аттестация		Промежуточная аттестация
		мационной безопасности»	6-7	
Тема 7. Сертификация и лицензирование	ОК 1, ОК 4, ОК 5, ОК 8, ПК.3.3, У2	Практическая работа № 10 «Заполнение заявления на сертификацию средства защиты информации»		

1. Устный зачет по Теме 1

Инструкция для обучающихся: Зачет сдается в рамках учебного занятия. Каждому студенту по выбору преподавателя дается два вопроса, на которые он отвечает в устной форме.

Выполнение задания: одному студенту на ответ выделяется 3 мин, группа сдает зачет за одно учебное занятие.

Вопросы к зачету:

1. Понятие КИИ, компоненты КИИ
2. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.
3. Категорирование объектов КИИ
4. Реестр значимых объектов КИИ
5. Оценка безопасности КИИ

Эталоны ответов: приведены в Учебном пособие по дисциплине «Основы информационной безопасности».

2. Практическая работа № 2
«Классификация угроз информационной безопасности»

Инструкция для обучающихся

Внимательно прочитайте задание и определите угрозы информационной безопасности, которые обладают соответствующими характеристиками.

Время выполнения задания – 60 минут.

Задание:

1. Используя банк данных угроз ФСТЭК России, определите, какие угрозы были добавлены в банк в текущем году. Укажите название код угрозы, источник угроз и объекты воздействия.
2. Приведите 3 примеров гроз для каждого класса:

Класс угрозы	Наименование угрозы
Внешние угрозы	
Внутренние угрозы	
Угрозы нарушения конфиденциальности	
Угрозы нарушения целостности	
Угрозы нарушения доступности	
Антропогенные угрозы	

2. Определите название, название угрозы, источники угрозы, объекты воздействия и последствия угрозы по ее описанию.

1. Угроза заключается в возможности выявления слабых мест в криптографических алгоритмах или уязвимостей в реализующем их программном обеспечении. Данная угроза обусловлена слабостями криптографических алгоритмов, а также ошибками в программном коде криптографических средств, их сопряжении с системой или параметрах их настройки.	
название угрозы	
источники угрозы	
объекты воздействия	
последствия угрозы	
2. Реализация данной угрозы возможна при условии отсутствия механизмов резервирования средств обработки, хранения и передачи информации, входящих в состав облачной информационной системы	
название угрозы	
источники угрозы	
объекты воздействия	
последствия угрозы	
3. Угроза заключается в возможности сброса пользователем (нарушителем) состояния оперативной памяти (обнуления памяти) путём случайного или намеренного осуществления перезагрузки отдельных устройств, блоков или системы в целом.	
название угрозы	
источники угрозы	
объекты воздействия	
последствия угрозы	
3. Угроза заключается в возможности нарушения целостности защищаемой информации путём осуществления нарушителем деструктивного физического воздействия на машинный носитель информации или деструктивного программного воздействия (в	
название угрозы	
источники угрозы	
объекты воздействия	
последствия угрозы	
4. Угроза заключается в возможности нарушителя выдавать себя за легитимного пользователя и выполнять приём/передачу данных от его имени. Данную угрозу можно охарактеризовать как «имитация действий клиента».	
название угрозы	
источники угрозы	
объекты воздействия последствия угрозы	
последствия угрозы	
5. Угроза заключается в возможности извлечения паролей из оперативной памяти компьютера или хищения (копирования) файлов паролей (в том числе хранящихся в открытом виде) с машинных носителей информации.	
название угрозы	

источники угрозы	
объекты воздействия	
последствия угрозы	
6. Угроза заключается в возможности осуществления нарушителем практически любых деструктивных действий в отношении дискредитируемой информационной системы при получении им физического доступа к аппаратным средствам вычислительной	
название угрозы	
источники угрозы	
объекты воздействия	
последствия угрозы	
7. Угроза заключается в возможности осуществления внешним нарушителем кражи компьютера (и подключённых к нему устройств), USB-накопителей, оптических дисков или других средств хранения, обработки, ввода/вывода/передачи информации.	
название угрозы	
источники угрозы	
объекты воздействия	
последствия угрозы	
8. Угроза заключается в возможности внесения нарушителем изменений в журналы регистрации событий безопасности дискредитируемой системы (удаление компрометирующих нарушителя записей или подделка записей о не произошедших событиях)	
название угрозы	
источники угрозы	
объекты воздействия	
последствия угрозы	
9. Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к данным, содержащимся в буфере обмена, в интересах ознакомления с хранящейся там информацией или осуществления деструктивного программного	
название угрозы	
источники угрозы	
объекты воздействия	
последствия угрозы	

Эталон ответа

1. Используя банк данных угроз ФСТЭК России, определите, какие угрозы были добавлены в банк в текущем году. Укажите название код угрозы, источник угроз и объекты воздействия

УБИ.211: Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем
Источник угрозы Внутренний нарушитель с низким потенциалом
Объект воздействия Системное программное обеспечение

УБИ.217: Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения
Источники угрозы
Внутренний нарушитель со средним потенциалом
Внешний нарушитель со средним потенциалом
Объект воздействия Информационная система, файлы

УБИ.216: Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах
Источники угрозы
Внешний нарушитель со средним потенциалом
Объект воздействия Программное обеспечение (программы)

Класс угрозы	Наименование угрозы
Внешние угрозы	Угроза использования альтернативных путей доступа к ресурсам Угроза доступа/перехвата/изменения HTTP cookies Угроза несанкционированного восстановления удалённой защищаемой информации
Внутренние угрозы	Угроза воздействия на программы с высокими привилегиями Угроза искажения XML-схемы Угроза исследования механизмов работы программы
Угрозы нарушения конфиденциальности	Угроза автоматического распространения вредоносного кода в грид-системе Угроза использования информации идентификации/аутентификации, заданной по умолчанию Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг
Угрозы нарушения целостности	Угроза деструктивного изменения конфигурации/среды окружения программ Угроза изменения системных и глобальных переменных Угроза некачественного переноса инфраструктуры в облако
Угрозы нарушения доступности	Угроза загрузки нештатной операционной системы Угроза межсайтовой подделки запроса Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия
Антропогенные угрозы	Недобросовестные партнеры Потенциальные преступники и хакеры Криминальные структуры

2. Определите название, название угрозы, источники угрозы, объекты воздействия и последствия угрозы по ее описанию.

1. Угроза заключается в возможности выявления слабых мест в криптографических алгоритмах или уязвимостей в реализующем их программном обеспечении. Данная угроза обусловлена слабостями криптографических алгоритмов, а также ошибками в программном

коде криптографических средств, их сопряжении с системой или параметрах их настройки.	
название угрозы	УБИ.003: Угроза анализа криптографических алгоритмов и их реализации
источники угрозы	Внешний нарушитель со средним потенциалом
объекты воздействия	Метаданные, системное программное обеспечение
последствия угрозы	Нарушение конфиденциальности Нарушение целостности
2. Реализация данной угрозы возможна при условии отсутствия механизмов резервирования средств обработки, хранения и передачи информации, входящих в состав облачной информационной системы	
название угрозы	УБИ.142: Угроза приостановки оказания облачных услуг вследствие технических сбоев
источники угрозы	-
объекты воздействия	Системное программное обеспечение, аппаратное обеспечение, канал связи
последствия угрозы	Нарушение доступности
3. Угроза заключается в возможности сброса пользователем (нарушителем) состояния оперативной памяти (обнуления памяти) путём случайного или намеренного осуществления перезагрузки отдельных устройств, блоков или системы в целом.	
название угрозы	УБИ.113: Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники
источники угрозы	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом
объекты воздействия	Системное программное обеспечение, аппаратное обеспечение
последствия угрозы	Нарушение целостности Нарушение доступности
3. Угроза заключается в возможности нарушения целостности защищаемой информации путём осуществления нарушителем деструктивного физического воздействия на машинный носитель информации или деструктивного программного воздействия (в	
название угрозы	УБИ.179: Угроза несанкционированной модификации защищаемой информации
источники угрозы	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом
объекты воздействия	Объекты файловой системы
последствия угрозы	Нарушение целостности
4. Угроза заключается в возможности нарушителя выдавать себя за легитимного пользователя и выполнять приём/передачу данных от его имени. Данную угрозу можно охарактеризовать как «имитация действий клиента».	
название угрозы	УБИ.128: Угроза подмены доверенного пользователя
источники угрозы	Внешний нарушитель с низким потенциалом
объекты воздействия	Сетевой узел, сетевое программное обеспечение

ствия последствия угрозы	
последствия угрозы	Нарушение конфиденциальности
5. Угроза заключается в возможности извлечения паролей из оперативной памяти компьютера или хищения (копирования) файлов паролей (в том числе хранящихся в открытом виде) с машинных носителей информации.	
название угрозы	УБИ.074: Угроза несанкционированного доступа к аутентификационной информации
источники угрозы	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом
объекты воздействия	Системное программное обеспечение, объекты файловой системы, учётные данные пользователя, реестр, машинные носители информации
последствия угрозы	Нарушение конфиденциальности
6. Угроза заключается в возможности осуществления нарушителем практически любых деструктивных действий в отношении дискредитируемой информационной системы при получении им физического доступа к аппаратным средствам вычислительной	
название угрозы	УБИ.139: Угроза преодоления физической защиты
источники угрозы	Внешний нарушитель со средним потенциалом
объекты воздействия	Сервер, рабочая станция, носитель информации, аппаратное обеспечение
последствия угрозы	Нарушение конфиденциальности Нарушение целостности Нарушение доступности
7. Угроза заключается в возможности осуществления внешним нарушителем кражи компьютера (и подключённых к нему устройств), USB-накопителей, оптических дисков или других средств хранения, обработки, ввода/вывода/передачи информации.	
название угрозы	УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации
источники угрозы	Внешний нарушитель с низким потенциалом
объекты воздействия	Сервер, рабочая станция, носитель информации, аппаратное обеспечение
последствия угрозы	Нарушение конфиденциальности Нарушение доступности
8. Угроза заключается в возможности внесения нарушителем изменений в журналы регистрации событий безопасности дискредитируемой системы (удаление компрометирующих нарушителя записей или подделка записей о не произошедших событиях)	
название угрозы	УБИ.124: Угроза подделки записей журнала регистрации событий
источники угрозы	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом
объекты воздействия	Системное программное обеспечение
последствия угрозы	Нарушение целостности
9. Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к данным, содержащимся в буфере обмена, в интересах ознакомления с хранящейся	

там информацией или осуществления деструктивного программного	
название угрозы	УБИ.093: Угроза несанкционированного управления буфером
источники угрозы	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом
объекты воздействия	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение
последствия угрозы	Нарушение конфиденциальности Нарушение целостности Нарушение доступности

3. Практическая работа № 4
«Классификация информации по видам тайн и степеням конфиденциальности»

Инструкция для обучающихся

Внимательно прочитайте задание. Определите степень конфиденциальности приведенных сведений.

Время выполнения задания – 60 минут.

Задание:
1. Определите свой вариант в соответствии с указаниями преподавателя.
2. Выделите свой вариант цветом, остальные варианты удалите.
3. Распределите представленные ниже сведения по степени конфиденциальности и видам тайн: информация, доступ к которой нельзя ограничить, государственная тайна, персональные данные, коммерческая тайна, врачебная (медицинская) тайна, банковская тайна, адвокатская тайна, тайна страхования, тайна следствия и судопроизводства, служебная тайна, сведения о сущности изобретения.

Вариант 1

Сведения	Степень конфиденциальности информации, виды тайн
Сведения о страхователе	
Сведения о суждениях, имевших место при обсуждении и принятии решения, о позиции отдельных судей, входивших в состав суда	
Сведения о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов	
Чертежи	
Финансово-экономическая информация о деятельности организации	
Данные дактилоскопии	
Сведения о диагнозе заболевания	
Технология производства	
Информация о счетах клиентов	
Место прописки и проживания гражданина	
Информация, циркулирующая в органах государственной власти рай-	

Сведения	Степень конфиденциальности информации, виды тайн
онного уровня	
Сведения о состоянии окружающей среды	
Сведения, полученные налоговым органом	

Вариант 2

Сведения	Степень конфиденциальности информации, виды тайн
Финансово-экономическая информация о деятельности организации	
Банковские реквизиты организации (для юридических лиц)	
Сведения, полученные адвокатом от доверителя	
ИНН	
Факт открытия счета (счетов), его номер и дата открытия	
Информация о факте обращения за медицинской помощью	
Информация об образце продукции	
Состав уголовного дела	
Сведения о здоровье страхователя	
Сведения, связанные с оказанием адвокатом юридической помощи своему доверителю	
Информация, циркулирующая в органах государственной власти	
Нормативно-правое документы	
Сведения о запасах платины, металлов платиновой группы, природных алмазов в Государственном фонде драгоценных металлов и драгоценных камней Российской Федерации, Центральном банке Российской Федерации	

Вариант 3

Сведения	Степень конфиденциальности информации, виды тайн
Сведения об имущественном состоянии страхователя	
Сведения, полученные адвокатом от доверителя	
Паспортные данные гражданина	
Сведения о мерах государственной защиты	
Описание опытного образца продукции	
Информация, циркулирующая в органах местного самоуправления	
Сведения о деятельности органов государственной власти	
Сведения, полученные при обследовании и лечении гражданина	
Данные биометрии	
Сведения об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны	
Сведения о состоянии здоровья застрахованного лица	
Паспортные данные клиентов банка (для физических лиц)	
Финансово-экономическая информация о деятельности организации	

Вариант 4

Сведения	Степень конфиденциальности информации, виды тайн
Сведения о личности донора	
Сведения о методах и средствах защиты секретной информации	
Движение денежных средств на счетах и депозитных вкладах	
Финансово-экономическая информация о деятельности организации	
Фамилия, имя, отчество гражданина, сопровождаемые фотографией	
Полномочия органов государственной власти и местного самоуправления	
Сведения, связанные с оказанием адвокатом юридической помощи своему доверителю	
Информация о состоянии окружающей среды	
Информация, циркулирующая в органах государственной власти регионального уровня	
Описание (формула) изобретения	
Сведения о состоянии здоровья застрахованного лица	
Данные предварительного расследования	
Факт наличия кредита	

Эталон ответа

Вариант 1

Сведения	Степень конфиденциальности информации, виды тайн
Сведения о страхователе	Тайна страхования
Сведения о суждениях, имевших место при обсуждении и принятии решения, о позиции отдельных судей, входивших в состав суда	Тайна следствия и судопроизводства
Сведения о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов	Служебная тайна
Чертежи	Сведения о сущности изобретения
Финансово-экономическая информация о деятельности организации	Коммерческая тайна
Данные дактилоскопии	Персональные данные
Сведения о диагнозе заболевания	Медицинская тайна
Технология производства	Сведения о сущности изобретения
Информация о счетах клиентов	Банковская тайна
Место прописки и проживания гражданина	Персональные данные
Информация, циркулирующая в органах государственной власти районного уровня	Государственная тайна
Сведения о состоянии окружающей среды	Информация, доступ к которой нельзя ограничить
Сведения, полученные налоговым органом	Налоговая тайна

Вариант 2

Сведения	Степень конфиденциальности информации, виды тайн
Финансово-экономическая информация о деятельности организации	Коммерческая тайна
Банковские реквизиты организации (для юридических лиц)	Банковская тайна
Сведения, полученные адвокатом от доверителя	Адвокатская тайна
ИНН	Персональные данные
Факт открытия счета (счетов), его номер и дата открытия	Банковская тайна
Информация о факте обращения за медицинской помощью	Медицинская тайна
Информация об образце продукции	Сведения о сущности изобретения
Состав уголовного дела	Тайна следствия и судопроизводства
Сведения о здоровье страхователя	Тайна страхования
Сведения, связанные с оказанием адвокатом юридической помощи своему доверителю	Адвокатская тайна
Информация, циркулирующая в органах государственной власти	Государственная тайна
Нормативно-правое документы	Информация, доступ к которой нельзя ограничить
Сведения о запасах платины, металлов платиновой группы, природных алмазов в Государственном фонде драгоценных металлов и драгоценных камней Российской Федерации, Центральном банке Российской Федерации	Государственная тайна

Вариант 3

Сведения	Степень конфиденциальности информации, виды тайн
Сведения об имущественном состоянии страхователя	Тайна страхования
Сведения, полученные адвокатом от доверителя	Адвокатская тайна
Паспортные данные гражданина	Персональные данные
Сведения о мерах государственной защиты	Информация, доступ к которой нельзя ограничить
Описание опытного образца продукции	Коммерческая тайна
Информация, циркулирующая в органах местного самоуправления	Служебная тайна
Сведения о деятельности органов государственной власти	Информация, доступ к которой нельзя ограничить
Сведения, полученные при обследовании и лечении гражданина	Медицинская тайна
Данные биометрии	Персональные данные
Сведения об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны	Государственная тайна
Сведения о состоянии здоровья застрахованного лица	Тайна страхования
Паспортные данные клиентов банка (для физических лиц)	Персональные данные
Финансово-экономическая информация о деятельности организации	Коммерческая тайна

Вариант 4

Сведения	Степень конфиденциальности информации, виды тайн
Сведения о личности донора	Врачебная тайна
Сведения о методах и средствах защиты секретной информации	Служебная тайна
Движение денежных средств на счетах и депозитных вкладах	Банковская тайна
Финансово-экономическая информация о деятельности организации	Коммерческая тайна
Фамилия, имя, отчество гражданина, сопровождаемые фотографией	Персональные данные
Полномочия органов государственной власти и местного самоуправления	Информация, доступ к которой нельзя ограничить
Сведения, связанные с оказанием адвокатом юридической помощи своему доверителю	Адвокатская тайна
Информация о состоянии окружающей среды	Информация, доступ к которой нельзя ограничить
Информация, циркулирующая в органах государственной власти регионального уровня	Служебная информация
Описание (формула) изобретения	Сведения о сущности изобретения
Сведения о состоянии здоровья застрахованного лица	Тайна страхования
Данные предварительного расследования	Тайна следствия и судопроизводства
Факт наличия кредита	Банковская тайна

4. Устный зачет по Темам 2-3

Инструкция для обучающихся: Зачет сдается в рамках учебного занятия. Каждому студенту по выбору преподавателя дается два вопроса, на которые он отвечает в устной форме.

Выполнение задания: одному студенту на ответ выделяется 3 мин, группа сдает зачет за одно учебное занятие.

Вопросы к зачету:

1. Понятие угрозы информационной безопасности, виды угроз информационной безопасности.
2. Объекты воздействия угроз. Информационные ресурсы организации.
3. Источники угроз, цели угроз.
4. Понятие уязвимости. Виды уязвимостей.
5. Свойства информации с точки зрения ИБ.
6. Виды информации в зависимости от категории доступа.
7. Жизненный цикл конфиденциальной информации в процессе ее создания, обработки, передачи.

Эталоны ответов: приведены в Учебном пособие по дисциплине «Основы информационной безопасности».

5. Практическая работа № 5 «Работа с моделями доступа, определение степени конфиденциальности информации»

Инструкция для обучающихся

Внимательно прочитайте задание. Постройте модели доступа для организации в соответствии с приведенными правилами.

Время выполнения задания – 60 минут.

Задание 1

Постройте матрицу доступа на основании предложенных правил дискреционной модели:

Исходные данные:

Файловая структура:

\ FOtd1\ F11.txt
\ F12.txt
\ F13.txt
\ FOtd2\ F21.txt
\ F22.txt
\ F23.txt
\ FOtd3 \ F31.txt
\ F32.txt
\ F33.txt

Пользователи: User1, User2

В корпоративной системе определены следующие правила доступа:

User1 может читать файлы F11, F31, F22, F23, записывать F12, F33, F32, к а, к остальным файлам пользователь имеет полный доступ

User2 может читать файлы F13, F21, F11, F31, F22, F23, записывать F32, к остальным файлам пользователь имеет полный доступ.

Решение

С учетом исходных данных матрица доступа будет выглядеть следующим образом:

Задание 2

Исходные данные:

Файловая структура:

\ FOtd1\ F11.txt

\ F12.txt
\ F13.txt
\ FOtd2\ F21.txt
\ F22.txt
\ F23.txt
\ FOtd3 \ F31.txt
\ F32.txt
\ F33.txt

Пользователи: User1, User2

Уровни конфиденциальности субъектов и объектов:
общий доступ, конфиденциально, секретно, совершенно секретно.

User 1 имеет метку доступа Конфиденциально.

Определите метку доступа для второго пользователя и метки конфиденциальности для всех файлов файловой структуры в соответствии с правилами модели Белла — Лападулы

Субъект/объект	**Метка**	**Субъект/объект**	**Метка**
User1	конфиденциально	F22	
User2		F23	
F11		F31	
F12		F32	
F13		F33	
F21			

Приведите графическое обоснование.

Уровень доступа (конфиденциальности)	User1	Файлы	User2
Совершенно секретно			
Секретно			
Конфиденциально			
Общий доступ			

Эталон ответа

Задание 1

User	F11	F31	F22	F23	F12	F33	F32	F13	F21	F11	F31	F22	F23	F32

User1	чтение	чтение	чтение	чтение	запись	запись	запись	полный доступ	полный доступ	полный доступ	полный доступ	полный доступ	полный доступ	полный доступ
User2	полный доступ	полный доступ	полный доступ	полный доступ	полный доступ	полный доступ	полный доступ	чтение	чтение	чтение	чтение	чтение	чтение	запись

Задание 2

Субъект/объект	Метка	Субъект/объект	Метка
User1	*конфиденциально*	F22	общий доступ
User2	конфиденциально	F23	общий доступ
F11	общий доступ	F31	общий доступ
F12	секретно	F32	секретно
F13	конфиденциально	F33	секретно
F21	конфиденциально		

Приведите графическое обоснование.

Уровень доступа (конфиденциальности)	User1 Файлы	User2
Совершенно секретно		
Секретно	F12, F33, F32	
Конфиденциально	F13, F21	
Общий доступ	F11,F31,F22,F23	

6. Практическая работа № 7

«Определение внутренних угроз информационной безопасности»

Инструкция для обучающихся

Внимательно прочитайте задание. Определите, какие угрозы из списка являются внутренними.

Время выполнения задания – 60 минут.

Задание:

Определите, какие из представленных угроз относятся к внутренними и могут быть предотвращены путем применения DLP-системы.

№	Описание угрозы	Да/нет
1.	Несанкционированный доступ к локальному компьютеру	
2.	Печать документов, содержащих конфиденциальную информацию	
3.	Использование ПЭМИН	
4.	Доступ к защищаемым файлам с использованием обходного пути	
5.	Передача аутентификационной информации	
6.	Загрузка нештатной операционной системы	
7.	Передача сведений конфиденциального характера по электронной почте	
8.	Обход многофакторной аутентификации	
9.	Несанкционированное использование привилегий	
10.	Несанкционированный съем аудиоинформации	
11.	Несанкционированная пересылка графических изображений	
12.	Использование недостатков языков программирования и ОС	
13.	Использование компьютерных вирусов	
14.	Публикация документов через web-сервисы	
15.	Маскировка под зарегистрированного пользователя	
16.	Несанкционированное копирования защищаемой информации	
17.	Внедрение вредоносного ПО	
18.	Кража носителей информации	
19.	Подключение несанкционированных носителей информации	
20.	Дистанционное фотографирование	
21.	Несанкционированная передача конфиденциальной информации по беспроводным каналам	
22.	Применение подслушивающих устройств	
23.	Подключение сетевых устройств	
24.	Несанкционированная передача файлов в облачное хранилище.	
25.	Доступ к несанкционированным носителям информации	
26.	Конфликт юрисдикций различных стран	
27.	Передача конфиденциальной информации по каналам мобильной связи	
28.	Несанкционированное восстановления аутентификационной информации	
29.	Попытки сделать скриншот	
30.	Вывод из строя аппаратного обеспечения	

Эталон ответа

№	Описание угрозы	Да/нет
31.	Несанкционированный доступ к локальному компьютеру	да
32.	Печать документов, содержащих конфиденциальную информацию	да
33.	Использование ПЭМИН	нет
34.	Доступ к защищаемым файлам с использованием обходного пути	нет

№	Описание угрозы	Да/нет
35.	Передача аутентификационной информации	да
36.	Загрузка нештатной операционной системы	да
37.	Передача сведений конфиденциального характера по электронной почте	да
38.	Обход многофакторной аутентификации	нет
39.	Несанкционированное использование привилегий	да
40.	Несанкционированный съем аудиоинформации	нет
41.	Несанкционированная пересылка графических изображений	да
42.	Использование недостатков языков программирования и ОС	нет
43.	Использование компьютерных вирусов	нет
44.	Публикация документов через web-сервисы	да
45.	Маскировка под зарегистрированного пользователя	нет
46.	Несанкционированное копирования защищаемой информации	да
47.	Внедрение вредоносного ПО	нет
48.	Кража носителей информации	нет
49.	Подключение несанкционированных носителей информации	да
50.	Дистанционное фотографирование	нет
51.	Несанкционированная передача конфиденциальной информации по беспроводным каналам	да
52.	Применение подслушивающих устройств	нет
53.	Подключение сетевых устройств	да
54.	Несанкционированная передача файлов в облачное хранилище.	да
55.	Доступ к несанкционированным носителям информации	да
56.	Конфликт юрисдикций различных стран	нет
57.	Передача конфиденциальной информации по каналам мобильной связи	да
58.	Несанкционированное восстановления аутентификационной информации	нет
59.	Попытки сделать скриншот	нет
60.	Вывод из строя аппаратного обеспечения	нет

7. Устный зачет по Темам 5-6

Инструкция для обучающихся: Зачет сдается в рамках учебного занятия. Каждому студенту по выбору преподавателя дается два вопроса, на которые он отвечает в устной форме.

Выполнение задания: одному студенту на ответ выделяется 3 мин, группа сдает зачет за одно учебное занятие.

Вопросы к зачету:

1. Направления защиты: правовая, организационная, техническая.
2. Подходы к обеспечению ИБ.
3. Физическая защита информации
4. Техническая защита информации
5. Криптографическая защита информации
6. Понятие и виды НСД, защита от НСД к информации.
7. Идентификация и аутентификация, виды аутентификации
8. Управление доступом. Модели доступа

9. Понятие DLP-системы. Структура, назначение, функции DLP-системы

Эталоны ответов: приведены в Учебном пособие по дисциплине «Основы информационной безопасности».

8. Практическая работа № 8

«Определение характеристик нарушителя ИБ в зависимости от угрозы информационной безопасности»

Инструкция для обучающихся

Внимательно прочитайте задание. Определите характеристики потенциального нарушителя.

Время выполнения задания – 60 минут.

Задание

Используя банк данных угроз ФСТЭК России, определить характеристики потенциального нарушителя в зависимости от угрозы

УБИ. 105	
Возможность физического доступа	
Уровень возможностей	
УБИ. 140	
Возможность физического доступа	
Уровень возможностей	
УБИ. 079	
Возможность физического доступа	
Уровень возможностей	
УБИ. 213	
Возможность физического доступа	
Уровень возможностей	
УБИ. 028	
Возможность физического доступа	
Уровень возможностей	

УБИ. 046	
Возможность физического доступа	
Уровень возможностей	
УБИ. 069	
Возможность физического доступа	
Уровень возможностей	
УБИ. 135	
Возможность физического доступа	
Уровень возможностей	
УБИ. 085	
Возможность физического доступа	
Уровень возможностей	
УБИ. 180	
Возможность физического доступа	

Эталон ответа

УБИ. 105	
Возможность физического доступа	Нет возможности. Реализация данной угрозы возможна при условии поступления запроса на загрузку в хранилище входных данных неизвестного формата.
Уровень возможностей	Внутренний нарушитель с низким потенциалом.
УБИ. 140	
Возможность физического доступа	Нет возможности. Угроза заключается в возможности отказа дискредитированной системой в доступе легальным пользователям при лавинообразном увеличении числа сетевых соединений с данной системой или при использовании недостатков реализации сетевых протоколов.
Уровень возможностей	Внутренний нарушитель с низким потенциалом. Внешний нарушитель с низким потенциалом.
УБИ. 079	
Возможность физического доступа	Нет возможности. Угроза заключается в возможности осуществления деструктивного программного воздействия на защищаемые виртуальные машины со стороны других виртуальных машин с помощью различных механизмов обмена данными между вирту-

	альными машинами, реализуемых гипервизором и активированных в системе.
Уровень возможностей	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом
УБИ. 213	
Возможность физического доступа	Есть возможность. Угроза заключается в возможности обхода многофакторной аутентификации путем внедрения вредоносного кода в дискредитируемую систему и компоненты, участвующие в процедуре многофакторной аутентификации.
Уровень возможностей	Внешний нарушитель с высоким потенциалом
УБИ. 028	
Возможность физического доступа	Есть возможность. Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемой информации в обход штатных механизмов с помощью нестандартных интерфейсов (в том числе доступа через командную строку в обход графического интерфейса).
Уровень возможностей	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом
УБИ. 046	
Возможность физического доступа	Нет возможности. Угроза заключается в возможности подмены субъекта виртуального информационного взаимодействия, а также в возможности возникновения состояния неспособности осуществления такого взаимодействия.
Уровень возможностей	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом
УБИ. 069	
Возможность физического доступа	Нет возможности. Угроза заключается в возможности внесения нарушителем изменений в работу сетевых протоколов путём добавления или удаления данных из информационного потока с целью оказания влияния на работу дискредитируемой системы или получения доступа к конфиденциальной информации, передаваемой по каналу связи.
Уровень возможностей	Внешний нарушитель с низким потенциалом
УБИ. 135	
Возможность физического доступа	Нет возможности. Угроза заключается в возможности нарушения конфиденциальности, целостности и доступности защищаемой информации потребителей облачных услуг, обрабатываемой в облачной системе.
Уровень возможностей	Внутренний нарушитель с низким потенциалом
УБИ. 085	

Возможность физического доступа	Нет возможности. Угроза заключается в возможности нарушения конфиденциальности информации, содержащейся в распределённых файлах, содержащих защищаемую информацию, путём восстановления данных распределённых файлов из их множества отдельных фрагментов с помощью программного обеспечения и информационных технологий по обработке распределённой информации.
Уровень возможностей	Внутренний нарушитель со средним потенциалом Внешний нарушитель со средним потенциалом
УБИ. 180	
Возможность физического доступа	Есть возможность. Угроза заключается в возможности повреждения части компонентов системы или системы в целом вследствие выхода температурного режима их работы из заданных требований из-за возникновения отказа входящих в неё подсистем вентиляции и температурных приборов.
Уровень возможностей	Внутренний нарушитель с низким потенциалом Внешний нарушитель со средним потенциалом

9. Практическая работа № 10

«Заполнение заявления на сертификацию средства защиты информации»

Инструкция для обучающихся

Внимательно прочитайте задание. Заполните заявление о продлении срока действующего сертификата средства защиты информации.

Время выполнения задания – 60 минут.

Задание

Используя Положение о системе сертификации средств защиты информации и данные Государственного реестра сертифицированных средств защиты информации и другую информацию официального сайта ФСТЭК России, заполните заявление о продлении срока действующего сертификата средства защиты информации.

Федеральная служба по техническому и экспортному контролю

ЗАЯВКА

на_____
(сертификацию средства защиты информации, продление срока действия сертификата соответствия)

Наименование средства защиты информации: _____

Назначение средства защиты информации: _____
степень секретности защищаемой информации, категория объекта информатизации, тип и класс защищенности информационной (автоматизированной) системы

Заявитель: _____
организационно-правовая форма и наименование

Адрес местонахождения заявителя: _____

Почтовый адрес заявителя: _____

Лицензии ФСТЭК России, имеющиеся у заявителя: _____
номера и даты выдачи лицензий

Ф.И.О. руководителя заявителя: _____

Ф.И.О. лица, ответственного за сертификацию средства защиты информации: _____

Контактный телефон (телефоны) заявителя: _____

Адрес электронной почты заявителя: _____

Разработчик (разработчики) средства защиты информации

(при наличии разработчика средства защиты информации):	_____ наименование, адрес местонахождения
Лицензии ФСТЭК России, имеющиеся у разработчика (разработчиков) средства защиты информации:	_____ номера и даты выдачи лицензий
Правообладатель (правообладатели) средства защиты информации (при наличии правообладателя (правообладателей) средства защиты информации):	_____ наименование лица (лиц), обладающего (обладающих) исключительными правами на средство защиты информации, адрес его (их) местонахождения
Испытательная лаборатория:	_____ наименование, адрес местонахождения
Тип средства защиты информации:	_____ наименование типа (наименования типов) средства защиты информации
Требования по безопасности информации:	_____ наименования документов, на соответствие которым планируется проводить сертификацию средства защиты информации
Схема сертификации средства защиты информации:	_____
Заявляемый срок действия сертификата соответствия	_____
Место проведения сертификационных испытаний:	_____ адрес места (адреса мест) проведения сертификационных испытаний, наименование лица, на материально-технической базе которого планируется проводить сертификационные испытания средства защиты информации

Эталон ответа

ЗАЯВКА

на продление срока действия сертификата соответствия

(сертификацию средства защиты информации, продление срока действия сертификата соответствия)

Наименование средства защиты информации: TowerLane

Назначение средства защиты информации: Антивирусное ПО

Заявитель: ООО «АРЛЕН»

Адрес местонахождения заявителя: СПБ, ул. Учительская, д. 5

Почтовый адрес заявителя:	TowerLane @mail.ru
Лицензии ФСТЭК России, имеющиеся у заявителя:	№ 15838 С 23.03.2017
Ф.И.О. руководителя заявителя:	Антонов Антон Иванович
Ф.И.О. лица, ответственного за сертификацию средства защиты информации:	Ашутин Андрей Иванович
Контактный телефон (телефоны) заявителя:	+729772967
Адрес электронной почты заявителя:	ASCTLK@yandex.ru
Разработчик (разработчики) средства защиты информации (при наличии разработчика средства защиты информации):	ООО «БИК», Санкт-Петербург, ул. Авиационная, д. 7
Лицензии ФСТЭК России, имеющиеся у разработчика (разработчиков) средства защиты информации:	№518248, 20.05.2016
Правообладатель (правообладатели) средства защиты информации (при наличии правообладателя (правообладателей) средства защиты информации):	ООО «БИК», Санкт-Петербург, ул. Авиационная, д. 7
Испытательная лаборатория:	ЦКБИ ФГУП «СНПО «Элерон», Санкт-Петербург, ул. Авиационная, д. 1
Тип средства защиты информации:	Антивирус
Требования по безопасности информации:	Приказ ФСТЭК России от 11.02.2013 N 17
Схема сертификации средства защиты информации:	1
Заявляемый срок действия сертификата соответствия	1.10.2020
Место проведения сертификаци-	Санкт-Петербург, ул. Авиационная, д. 1

онных испытаний:

Приложение	— технические условия в двух экземплярах; — техническое задание в двух экземплярах — задание по безопасности в двух экземплярах — формуляр (паспорт) на средство защиты информации; — договор	
Должность руководителя заявителя (лица, которое в силу закона или учредительных документов выступает от его имени)	м.п. (при наличии) подпись	Антонов А. И. «21 » 04 2019 г.
Должность руководителя испытательной лаборатории	м.п. (при наличии) подпись	Крукин А. З. «23 »04 2019 г.

10. Устный зачет по Темам 7-8

Инструкция для обучающихся: зачет сдается в рамках учебного занятия. Каждому студенту по выбору преподавателя дается два вопроса, на которые он отвечает в устной форме.
Выполнение задания: одному студенту на ответ выделяется 3 мин, группа сдает зачет за одно учебное занятие.

Вопросы к зачету:

1. Понятие нарушителя ИБ, понятие модели нарушителя, характеристики нарушителя
2. Система сертификации средств защиты информации. Основные понятия.
3. Схемы сертификации. Государственный реестр сертифицированных средств защиты информации.
4. Порядок проведения сертификации.
5. Лицензирование в области защиты информации. Основные понятия.

Эталоны ответов: приведены в Учебном пособие по дисциплине «Основы информационной безопасности».

3.2. Контрольно-оценочные материалы для промежуточной аттестации по дисциплине

Формой промежуточной аттестации по дисциплине является **экзамен.**

Перечень экзаменационных вопросов:

№ п/п	Перечень теоретических вопросов
1.	Понятие КИИ. Компоненты КИИ.
2.	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ
3.	Категорирование объектов КИИ
4.	Реестр значимых объектов КИИ. Система безопасности значимого объекта КИИ. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры
5.	Понятие угрозы, виды угроз, объекты угроз, источники угроз. Банк данных угроз безопасности информации ФСТЭК России.
6.	Понятие уязвимости, классификация уязвимостей. Реестр уязвимостей ФСТЭК России.
7.	Виды информации в зависимости от категории доступа. Конфиденциальная информация.
8.	Жизненный цикл конфиденциальной информации в процессе ее создания, обработки, передачи.
9.	Подходы к обеспечению ИБ. Направления защиты информации.
10.	Средства защиты информации: физические, технические, криптографические.
11.	Понятие и виды НСД. Защита от НСД к информации. Способы реализации НСД.
12.	Идентификация и аутентификация.
13.	Управление доступом. Модели доступа
14.	Системы обнаружения вторжений (СОВ). Требования к СОВ.
15.	Понятие DLP-системы. Структура, назначение, функции DLP-системы.
16.	Вредоносное программное обеспечение
17.	Понятие нарушителя ИБ. Модели нарушителя ИБ
18.	Система сертификации средств защиты информации. Схемы сертификации. Государственный реестр сертифицированных средств защиты информации.
19.	Порядок сертификации. Правила и документы сертификации.
20.	Лицензирование в области защиты информации.

Эталон устных ответов: приведены в Учебном пособие по дисциплине «Основы информационной безопасности».

Условия выполнения

1. Количество билетов для экзаменующегося: 1
2. Время подготовки к ответу: 30 минут
3. Требования к устным ответам:
   Полное овладение содержанием учебного материала, в котором обучающийся легко ориентируется, владение понятийным аппаратом.
4. Оборудование: учебная аудитория, стол, стул, пишущая ручка, бумага.

Результаты промежуточной аттестации фиксируются в протоколе.

Критерии оценки устных ответов

В системе оценки знаний и умений используются **следующие критерии**:

«Отлично» – за глубокое и полное овладение содержанием учебного материала, в котором обучающийся легко ориентируется, владение понятийным аппаратом за умение связывать теорию с практикой, решать практические задачи, высказывать и обосновывать свои суждения. Отличная отметка предполагает грамотное, логичное изложение ответа (как в устной, так и в письменной форме), качественное внешнее оформление.

«Хорошо» – если обучающийся полно освоил учебный материал, владеет понятийным аппаратом, ориентируется в изученном материале, грамотно излагает ответ, но содержание и форма ответа имеют некоторые неточности.

«Удовлетворительно» – если обучающийся обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности в определение понятий, не умеет доказательно обосновать свои суждения.

«Неудовлетворительно» – если обучающийся имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определение понятий, искажает их смысл, беспорядочно и неуверенно излагает материал, за полное незнание и непонимание учебного материала или отказ отвечать.