Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

«УТВЕРЖДАЮ»
И.о. проректора
_____ А.В. Троицкий
_____ 2023 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ «ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ»

Специальность: 38.05.01 «Экономическая безопасность»
Специализация: «Экономико-правовое обеспечение экономической безопасности»
Уровень высшего образования: специалитет
Квалификация (степень) выпускника: экономист
Форма обучения очная, заочная

Королев
2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор: Сухотерин А.И.. Рабочая программа дисциплины: «Защита конфиденциальной информации». – Королев МО: «Технологический университет», 2023.

Рецензент: **к.в.н., доцент Воронов А.Н.**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по специальности 38.05.01 «Экономическая безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол **№ 9 от 11 апреля 2023 г.**

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	Сахнов В.Н. к.в.н., доцент				
Год утверждения (переутверждения)	2023	2024	2025	2026	2027
Номер и дата протокола заседания кафедры	№ 8 от 29.03.2023 г.				

Рабочая программа согласована:
Руководитель ОПОП _____ Коба Е.Е., к.э.н., доцент

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023	2024	2025	2026	2027
Номер и дата протокола заседания УМС	№ 5 от 11.04.2023 г.				

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП

Целями изучения дисциплины является:

- формирование у студентов специализированной базы знаний по основным понятиям в области системных и прикладных вопросов защиты конфиденциальной информации;
- усовершенствовать навыки по основам практического обоснования требований к системе защиты конфиденциальной информации, что позволит студенту ориентироваться на рынке средств информационной защиты при выборе оптимального решения.

В процессе обучения студент приобретает и совершенствует следующие компетенции:

Универсальные компетенции:

- УК-1- Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий;

Общепрофессиональные компетенции:

- ОПК-7. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности;

Профессиональные компетенции:

- ПК-4- Способен создавать организационно-управленческую и информационную структуру интегральной системы управления рисками, осуществлять координацию работ по технико-информационному обеспечению системы стратегического управления рисками

Показатель освоения компетенции отражают следующие индикаторы:

Трудовые действия:

УК-1.1-Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними;

УК-1. И-2. Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению;

УК-1. И-3. Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников;

УК-1.И-4 Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов;

УК-1. И-5 Использует логико-методологический инструментарий для критической оценки современных концепций философского и социального характера в своей предметной области;

ОПК-7. И-1Имеет представление, понимает принципы работы современных информационных технологий в экономике, программных средств для поиска, аккумулирования, хранения, обработки, анализа, планирования, оценки и передачи данных при решении профессиональных задач

ОПК-7. И-2 Ставит задачу для решения экономических задач, понимая специфику применения

информационных технологий
ОПК-7- И-1 Понимает алгоритмы работы разных поисковых систем и особенности составления запросов при поиске информации в сети Интернет и базах данных
ПК-4. И-1Создает организационно-управленческую и информационную структуру интегральной системы управления рисками, разрабатывает проекты нормативных и методических материалов, регламентирующих работу по защите информации, предлагает технологии защиты информации, безопасную систему внутренней и внешней коммуникации и отчетности;
ПК-4. И-2 Координирует работы по технико-информационному обеспечению системы стратегического управления рисками, анализирует информацию об уровне и тенденциях развития технико-информационного обеспечения системы управления рисками в отрасли и в организации, оценивает ресурсные затраты на внедрение и функционирование технико-информационной составляющей и эффективность внедрения автоматизированных информационных систем, управляет проектами технико-информационного обеспечения системы управления рисками;
ПК-4.И-3 Использует современные принципы, методы и технологии работы с информацией, принципы и методы управления проектами, положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности;
ПК-4.И-4 Применяет в профессиональной деятельности современные информационные технологии, используемые в сфере управления рисками, работает с различными информационными ресурсами и технологиями, использует программные обеспечения для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных) на уровне опытного пользователя.

Необходимые умения:

УК-1И-1.У-1 Умеет проводить анализ проблемной ситуации как системы, выявляя ее составляющие и связи между ними;
УК-1. И-2. У-1 Умеет определять пробелы в информации, необходимой для решения проблемной ситуации;
УК-1. И-2. У-2 Умеет проектировать процессы по устранению пробелов в информации;
УК-1. И-3. У-1 Умеет критически оценивать надежность источников информации, работать с противоречивой информацией из разных источников;
УК-1.И-4.У-1 Умеет разрабатывать и аргументировать стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов
УК-1.И-5.У-1 Умеет использовать логико-методологический инструментарий для критической оценки современных концепций философского и социального характера в своей предметной области
ОПК-7. И-1. У-1 Умеет осуществлять поиск, аккумулирование, хранение, обработку, анализ, планирование, оценку и передачу данных при решении профессиональных задач с использованием современных информационных технологий
ОПК-7. И-2. У-1 Умеет интегрировать и перерабатывать цифровой контент для постановки и решения задачи путем анализа закрытых и открытых баз данных;
ОПК-7- И-1. У-1 Умеет составлять запрос и проанализировать извлеченные данные
ПК-4. И-1. У-1 Умеет создавать организационно-управленческую и информационную структуру интегральной системы управления рисками;
ПК-4. И-1. У-2 Умеет разрабатывать проекты нормативных и методических материалов, регламентирующих работу по защите информации,
ПК-4. И-1. У-3 Умеет осуществлять выбор средств и технологий защиты информации, безопасной системы внутренней и внешней коммуникации и отчетности
ПК-4. И-2. У-1 Умеет координировать работы по технико-информационному обеспечению системы стратегического управления рисками;
ПК-4. И-2. У-2 Умеет проводить анализ информации об уровне и тенденциях развития технико-информационного обеспечения системы управления рисками в отрасли и в организации,

ПК-4. И-2. У-3 Умеет оценивать ресурсные затраты на внедрение и функционирование технико-информационной составляющей и эффективность внедрения автоматизированных информационных систем, управляет проектами технико-информационного обеспечения системы управления рисками
ПК-4.И-3. У-1 Умеет использовать современные принципы, методы и технологии работы с информацией,
ПК-4.И-3. У-2 Умеет применять принципы и методы управления проектами,
ПК-4.И-3. У-3 Умеет использовать положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности
ПК-4.И-4. У-1 Умеет применять в профессиональной деятельности современные информационные технологии, используемые в сфере управления рисками
ПК-4.И-4. У-2 Умеет работать с различными информационными ресурсами и технологиями, программными обеспечениями для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных) на уровне опытного пользователя
ПК-4. И-5. У-1 Умеет использовать в профессиональной деятельности основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации, компьютерную технику, оснащенную альтернативными устройствами ввода-вывода информации, адаптивные технические средства для людей с ограниченными возможностями здоровья
ПК-4. И-6. У-1 Умеет решать поставленные задачи в области системных и прикладных вопросов защиты информации в системах электронного документооборота на основе действующего российского законодательства с помощью современных принципов, методов и средств в различных организационных структурах, по базовым направлениям защиты государственной и коммерческой тайны и конфиденциальной информации

Необходимые знания:
УК-1. И-1. З-1 . Знает методику проведения анализа проблемной ситуации как системы, знает ее составляющие и связи между ними
УК-1. И-2. З-1 Знает способы определения пробелов в информации, необходимой для решения проблемной ситуации;
УК-1. И-2. З-2 Знает алгоритм проектирования процессов по устранению пробелов в информации, необходимой для решения проблемной ситуации;
УК-1. И-3. З-1 Знает методы оценки надежности источников информации, порядок работы с противоречивой информацией из различных источников.
УК-1. И-4. З-1 Знает методику разработки стратегий решения проблемных ситуаций на основе системного и междисциплинарных подходов
УК-1. И-5. З-1 Знает современные концепции философского и социального характера в своей предметной области, методологический инструментарий для их критической оценки
ОПК-7. И-1. З-1 Знает принципы работы современных информационных технологий в экономике и программных средств
ОПК-7. И-2. З-1 Знает принципы классификации экономических задач в зависимости от типа экономических данных;
ОПК-7- И-1. З-1 Знает принципы работы и формирования запросов методом парсинга, используя базовые знания программирования.
ПК-4. И-1. З-1 Знает принципы создания организационно-управленческой и информационной структуры интегральной системы управления рисками;
ПК-4. И-1. З-2 Знает методические материалы, регламентирующие работу по защите информации,
ПК-4. И-1. З-3 Знает технологии защиты информации, безопасной системы внутренней и внешней коммуникации и отчетности
ПК-4. И-2. З-1 Знает требования к технико-информационному обеспечению управления рисками;

ПК-4. И-2. З-2 Знает современные информационные технологии, применяемые в управлении рисками
ПК-4. И-2. З-3 Знает бюджет организации на внедрение и поддержание технико-информационного обеспечения системы управления рисками
ПК-4.И-3. З-1 Знает современные принципы, методы и технологии работы с информацией
ПК-4.И-3. З-2 Знает принципы и методы управления проектами
ПК-4.И-3. З-3 Знает положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности
ПК-4.И-4. З-1 Знает различные информационные ресурсы и технологии, программные обеспечения для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных)
ПК-4. И-5. З-1 Знает основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации,
ПК-4. И-5. З-2 Знает принципы работы с компьютерной техникой, оснащенной альтернативными устройствами ввода-вывода информации, адаптивными техническими средствами для людей с ограниченными возможностями здоровья
ПК-4. И-6. З-1 Знает принципы и требования обеспечения сохранения государственной и коммерческой тайны и конфиденциальной информации;
ПК-4. И-6. З-2 Знает принципы работы в системах электронного документооборота;
ПК-4. И-6. З-3 Знает действующее российское законодательство в сфере защиты государственной и коммерческой тайны и конфиденциальной информации.

2. Место дисциплины в структуре ОПОП

Дисциплина относится к вариативной части дисциплин по выбору Блока 1 основной образовательной программы подготовки специалиста по направлению подготовки 38.05.01 «Экономическая безопасность», специализация: «Экономико-правовое обеспечение экономической безопасности». Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученной дисциплине: «Основы информационной безопасности», «Безопасность электронного документооборота», «Информационные технологии в профессиональной деятельности», «Адаптированные информационные технологии» и компетенциях УК-1; УК-9; ПК-4.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при изучении дисциплин: «Экономическая безопасность», «Информационно-аналитическая деятельность по обеспечению комплексной информационной безопасности», «Информационные системы в экономике», «Информационная безопасность предприятия» и выполнении выпускной квалификационной работы специалиста.

3. Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины для студентов очной и очно-заочной формы составляет 3 зачетных единиц, 108 часов.

Виды занятий	**Всего часов**	**Семестр**	**Семестр** 4	**Семестр 5**	**Семестр …**
Общая трудоемкость	**108**		**108**	**108**	

ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**48**		**48**		
Лекции (Л)	**16**		**16**		
Практические занятия (ПЗ)	**32**		**32**		
Лабораторные работы (ЛР)	**нет**		**нет**		
Самостоятельная работа	**60**		**60**		
Практическая подготовка	нет		нет		
Курсовые работы (проекты)	**-**		**-**		
Расчетно-графические работы	**-**		**-**		
Контрольная работа, домашнее задание	+ -		+ -		
Текущий контроль знаний	**Тесты**		**Тесты**		
Вид итогового контроля	**Экзамен**		**Экзамен**		
ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**16**			**16**	
Лекции (Л)	**4**			**4**	
Практические занятия (ПЗ)	**8**			**8**	
Лабораторные работы (ЛР)	**нет**			**нет**	
Практическая подготовка	**нет**			**нет**	
Самостоятельная работа	**92**			**92**	
Курсовые работы (проекты)	**-**			**-**	
Расчетно-графические работы	**-**			**-**	
Контрольная работа, домашнее задание	**+** **-**			**+** **-**	
Вид итогового контроля	**Экзамен**			**Экзамен**	

4. Содержание дисциплины

4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. очное/заочное	Практические занятия, час. очное/заочное	Занятия в интерактивной форме, час. очное/заочное	Код компетенций
Тема 1: Технология контроля санкционированных событий. Парольная аутентификация	1/0.4	3/0.5	2/0.5	**УК-1;**
Тема 2: Методы биометрической идентификации и анализ эффективности их	1/0.4	3/0.5	2/0.5	**УК-1;**

использования для ограничения доступа. Аутентификация с помощью биометрических характеристик				
Тема 3: Аутентификация с помощью одноразовых паролей	1/0.4	3/0.5	2/0.5	**УК-1; ОПК-7;**
Тема 4:Криптография с открытым ключом	1/0.4	3/0.5	2/0.5	**УК-1; ОПК-7;**
Тема 5:Протоколы аутентификации в локальной сети	2/0.4	3/1	3/1	**УК-1; ОПК-7;**
Тема 6:Механизмы аутентификации при осуществлении подключений	2/0.4	3/1	3/1	**УК-1; ОПК-7; ПК-4**
Тема 7:Аутентификация в защищенных соединениях	2/0.4	3/1	3/1	**УК-1; ОПК-7; ПК-4**
Тема 8:Применение метода димензиональной онтологии при выборе средств технической защиты информации от несанкционированного доступа. Применение аппаратных средств аутентификации и хранения ключевой информации	2/0.4	3/1	5/1	**УК-1; ОПК-7; ПК-4**
Тема 9. Практическая реализация механизмов добавочной защиты	2/0.4	4/1	6/1	**УК-1; ОПК-7; ПК-4**
Тема 10. Разработка и оптимизация механизма уровневого контроля, как механизма реального времени	2/0.4	4/1	6/1	**УК-1; ОПК-7; ПК-4**
Итого:	16/4	32/8	34/8	

4.2. Содержание тем дисциплины

Раздел I. Обеспечение безопасного допуска к информационным ресурсам

Тема 1. Технология контроля санкционированных событий. Парольная аутентификация

Возможности СЗИ НСД. Изменение уровня защищенности во времени. Метод контроля санкционированных событий. Технология контроля санкционированных событий. Дополнительные возможности механизма. Расширение возможностей, механизма контроля целостности файловых объектов. Двухуровневая модель аудита.

Основные понятия и определения. Роль и задачи аутентификации. Место аутентификации в структуре основных направлений защиты информации. Факторы аутентификации. Аутентификация с помощью запоминаемого пароля. Ме-

тоды парольной аутентификации. Парольные политики. Недостатки методов аутентификации с запоминаемым паролем.

Тема 2. Аутентификация с помощью биометрических характеристик

Биометрические характеристики. Как работают биометрические системы.

Аутентификация и биометрическое распознавание. Реализация биометрических систем. Недостатки аутентификации с помощью биометрических характеристик. Возможные атаки.

Тема 3. Аутентификация с помощью одноразовых паролей

Аппаратно – программные OTP - токены. Как работают OTP – токены. Методы аутентификации с помощью OTP – токенов. Сравнение методов OTP – аутентификации. Системы одноразовых паролей. Недостатки методов аутентификации с помощью OTP. Возможные атаки.

Тема 4. Криптография с открытым ключом

Общие сведения о криптографии с открытым ключом. Авторизация и обеспечение юридической значимости электронных документов. Конфиденциальность и контроль целостности передаваемой информации. Аутентификация связывающихся сторон. Установление аутентичного защищаемого соединения. Инфраструктура открытых ключей (PKI). Аутентификация с помощью открытого ключа на основе сертификатов. Организация хранения закрытого ключа. Интеллектуальные устройства и аутентификация с помощью открытого ключа. Недостатки аутентификации с помощью открытых ключей. Возможные атаки.

Тема 5. Протоколы аутентификации в локальной сети

Протоколы LAN Manager и NT LAN Manager. Протокол Kerberos. Протокол Kerberos + PKINIT.

Тема 6. Механизмы аутентификации при осуществлении подключений

Протокол PPP PAP. Протокол PPP CHAP. Протокол PPP EAP. Протокол TACACS+. Протокол RADIUS. Стандарт IEEE 802.1x и протокол EAPOL. Протокол EAP- TLS с использованием российской криптографии. Стандарт IEEE 802.1x в операционных системах Microsoft. Cisco NAC.

Тема 7. Аутентификация в защищенных соединениях

Протоколы SSL, TSL. Протокол SSH. Протоколы S-HTTP. Протокол SOCKS. Протокол IPSec. Протоколы защищенного взаимодействия и аутентификации для корпоративных беспроводных локальных сетей.

Тема 8. Применение метода димензиональной онтологии при выборе средств технической защиты информации от несанкционированного доступа. Применение аппаратных средств аутентификации и хранения ключевой информации

Применение метода димензиональной онтологии при выборе средств технической защиты информации от несанкционированного доступа.

Аппаратные средства защиты в современных PKI решениях. Необходимость применения аппаратных средств аутентификации и хранения ключевой информации. Типовые требования к средствам аутентификации и хранения ключевой информации. Особенности корпоративного использования персональных средств аутентификации и хранения ключевой информации. Централизованная система управления средствами аутентификации и хранения ключевой информации пользователей. Типовые требования к системе управления токенами. Token Management System (TMS) компании Aladdin. Практика: комплексная система на базе единого персонального средства аутентификации и хранения ключевой информации.

Раздел II. Учет субъектов доступа. Реализация механизмов защиты

Тема 9. Практическая реализация механизмов добавочной защиты

Режим хранения КД. Порядок обращения с КД. Назначение, виды и принципы проведения проверок наличия КД. Проверки правильности проставления регистрационных данных конфиденциальных носителей, документов, дел и учетных журналов (карточек).

Тема 10. Разработка и оптимизация механизма уровневого контроля, как механизма реального времени

Проверки правильности проставления отметок о движении КД, дел и носителей. Квартальные проверки фактического наличия КД и документов. Годовая проверка наличия КД, документов выделенного хранения и учетных журналов (карточек). Не регламентные проверки наличия конфиденциальных носителей, документов и дел.

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Защита информации от несанкционированного доступа» приведена в Приложении 1.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

1. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ИНФРА-М, 2022. — 256 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016535-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1861659 (дата обращения: 03.10.2022). – Режим доступа: по подписке.

2. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. - Новосибирск : Изд-во НГТУ, 2019. - 83 с. - ISBN 978-5-7782-3918-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1866895 (дата обращения: 03.10.2022). – Режим доступа: по подписке.

Дополнительная литература:

1. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: https://doi.org/10.29039/01848-4. - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232287 (дата обращения: 03.10.2022). – Режим доступа: по подписке.

2. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: 60x90 1/16. - (Высшее образование: Бакалавриат; Магистратура). (переплет) ISBN 978-5-369-01378-6http://znanium.com/bookread2.php?book=474838

3. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429070

4. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2016 - 120 с.: 60x88 1/16 + (Доп. мат. znanium.com). - (Высшее образование: Бакалавр.). (о) ISBN 978-5-369-01379-3http://znanium.com/bookread2.php?book=549914

5. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие / Наталия Васильевна. – 2 ; доп. – М.: Издательство «ФОРУМ» : ООО «Научно-издательский центр ИНФРА-М», 2016. – 240 с. – ISBN 978-5-00091-007-8. URL: http://znanium.com/go.php?id=544554

Загинайлов, Ю. Н. Основы информационной безопасности : курс визуальных лекций / Ю. Н. Загинайлов ; Ю.Н. Загинайлов. - М. |Берлин : Директ-Медиа, 2015. - 105 с. - ISBN 978-5-4475-3947-4.
URL: http://biblioclub.ru/index.php?page=book&id=362895

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp** – научно-образовательный портал;
2. **http://informika.ru/** – образовательный портал;
3. **www.wikIsec.ru** - Энциклопедия информационной безопасности. – Публикации, статьи;
4. **www.biblioclub.ru** - Универсальная библиотека онлайн;
5. **www.rucont.ru** - ЭБС «Руконт»;
6. **http://www.academy.it.ru/** – академия АЙТИ;
7. **http://www.minfin.ru** - Официальный сайт Министерства финансов Российской Федерации;
8. **http://www.gov.ru/** - Официальный сервер органов государственной власти Российской Федерации;
9. **http://www.fsb.ru/** - Официальный сайт Федеральной Службы Безопасности;
10. **http://www.fstec.ru/** - Официальный сайт Федеральной Службы по Техническому Экспортному Контролю;
11. **http://www.minfin.ru** - Официальный сайт Министерства финансов Российской Федерации;
12. **http://www.gov.ru** - Официальный сервер органов государственной власти Российской Федерации;
13. **http://www.fsb.ru/** - Официальный сайт Федеральной Службы Безопасности;
14. **http://www.fstec.ru/** - Официальный сайт Федеральной Службы по Техническому Экспортному контролю.

9. Методические указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины приведены в Приложении 2 к настоящей рабочей программе.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

- **Перечень программного обеспечения:** MSOffice.
- **Информационные справочные системы:**

1. Ресурсы информационно-образовательной среды Университета.
2. Рабочая программа и методическое обеспечение по дисциплине: «Защита конфиденциальной информации»

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы:

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система WindowsXP; офисные программы MS Office 7;
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Приложение 1

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Специальность: 38.05.01 Экономическая безопасность

Специализация: Экономико-правовое обеспечение экономической безопасности

Квалификация (степень) выпускника: экономист

Форма обучения: очная, заочная

Королев
2023

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компетенции	Содержание компетенции (или ее части)*	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (или ее части), обучающийся должен:		
				Трудовые действия	необходимые умения	Необходимые знания
1.	УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий;	Тема:1,2,3,4, 5-10	УК-1.1-Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними; УК-1. И-2. Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению; УК-1. И-3. Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источни-	УК-1И-1.У-1 Умеет проводить анализ проблемной ситуации как системы, выявляя ее составляющие и связи между ними; УК-1. И-2. У-1 Умеет определять пробелы в информации, необходимой для решения проблемной ситуации; УК-1. И-2. У-2 Умеет проектировать процессы по устранению пробелов в информации; УК-1. И-3. У-1 Умеет критически оценивать надежность источников информа-	УК-1. И-1. З-1 . Знает методику проведения анализа проблемной ситуации как системы, знает ее составляющие и связи между ними УК-1. И-2. З-1 Знает способы определения пробелов в информации, необходимой для решения проблемной ситуации; УК-1. И-2. З-2 Знает алгоритм проектирования процессов по устранению пробелов в информации, необходимой для решения проблемной ситуации; УК-1. И-3. З-1 Знает методы оценки надежности источников информации, порядок работы с противоречивой информацией из различных источников. УК-1. И-4. З-1 Знает методику разработки стратегий решения про-

				ков; УК-1.И-4 Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов; УК-1. И-5 Использует логико-методологический инструментарий для критической оценки современных концепций философского и социального характера в своей предметной области;	ции, работать с противоречивой информацией из разных источников; УК-1.И-4.У-1 Умеет разрабатывать и аргументировать стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов УК-1.И-5.У-1 Умеет использовать логико-методологический инструментарий для критической оценки современных концепций философского и социального характера в своей предметной области	блемных ситуаций на основе системного и междисциплинарных подходов УК-1. И-5. З-1 Знает современные концепции философского и социального характера в
2.	ОПК-7	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	Тема:1,2,3,4,5-10	ОПК-7. И-1Имеет представление, понимает принципы работы современных информационных технологий в экономике, программных средств	ОПК-7. И-1. У-1 Умеет осуществлять поиск, аккумулирование, хранение, обработку, анализ, планирование, оценку и передачу данных при решении	ОПК-7. И-1. З-1 Знает принципы работы современных информационных технологий в экономике и программных средств

				для поиска, аккумулирования, хранения, обработки, анализа, планирования, оценки и передачи данных при решении профессиональных задач ОПК-7. И-2 Ставит задачу для решения экономических задач, понимая специфику применения информационных технологий ОПК-7- И-1 Понимает алгоритмы работы разных поисковых систем и особенности составления запросов при поиске информации в сети Интернет и базах данных	профессиональных задач с использованием современных информационных технологий ОПК-7. И-2. У-1 Умеет интегрировать и перерабатывать цифровой контент для постановки и решения задачи путем анализа закрытых и открытых баз данных; ОПК-7- И-1. У-1 Умеет составлять запрос и проанализировать извлеченные данные	ОПК-7. И-2. З-1 Знает принципы классификации экономических задач в зависимости от типа экономических данных; ОПК-7- И-1. З-1 Знает принципы работы и формирования запросов методом парсинга, используя базовые знания программирования.
3.	ПК-4	Способен создавать организационно-управленческую и информационную структуру интегральной системы управления рисками, осуществлять координацию работ по технико-информационному обеспечению системы стратегического управления рисками	Тема:1,2,3,4,5-10	ПК-4. И-1 Создает организационно-управленческую и информационную структуру интегральной системы управления рисками, разрабатывает проекты нормативных и методических материалов, регламентирующих работу по защите информации, предлагает технологии защиты информации, безопасную систему внутренней и внешней коммуникации и отчетности ПК-4. И-2	ПК-4. И-1. У-1 Умеет создавать организационно-управленческую и информационную структуру интегральной системы управления рисками; ПК-4. И-1. У-2 Умеет разрабатывать проекты нормативных и методических материалов, регламентирующих работу по защите информации, ПК-4. И-1. У-3 Умеет осуществлять выбор средств и технологий защиты информации, без-	ПК-4. И-1. З-1 Знает принципы создания организационно-управленческой и информационной структуры интегральной системы управления рисками; ПК-4. И-1. З-2 Знает методические материалы, регламентирующие работу по защите информации, ПК-4. И-1. З-3 Знает технологии защиты информации, безопасной системы внутренней и внешней коммуникации и отчет-

				Координирует работы по технико-информационному обеспечению системы стратегического управления рисками, анализирует информацию об уровне и тенденциях развития технико-информационного обеспечения системы управления рисками в отрасли и в организации, оценивает ресурсные затраты на внедрение и функционирование технико-информационной составляющей и эффективность внедрения автоматизированных информационных систем, управляет проектами технико-информационного обеспечения системы управления рисками ПК-4.И-3 Использует современные принципы, методы и технологии работы с информацией, принципы и методы управления проектами, положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопас-	опасной системы внутренней и внешней коммуникации и отчетности ПК-4. И-2. У-1 Умеет координировать работы по технико-информационному обеспечению системы стратегического управления рисками; ПК-4. И-2. У-2 Умеет проводить анализ информации об уровне и тенденциях развития технико-информационного обеспечения системы управления рисками в отрасли и в организации, ПК-4. И-2. У-3 Умеет оценивать ресурсные затраты на внедрение и функционирование технико-информационной составляющей и эффективность внедрения автоматизированных информационных систем, управляет проектами технико-информационного обеспечения системы управления рисками ПК-4.И-3. У-1 Умеет использовать современные принципы, методы и технологии работы с информацией, ПК-4.И-3. У-2 Умеет применять принципы	ности ПК-4. И-2. З-1 Знает требования к технико-информационному обеспечению управления рисками; ПК-4. И-2. З-2 Знает современные информационные технологии, применяемые в управлении рисками ПК-4. И-2. З-3 Знает бюджет организации на внедрение и поддержание технико-информационного обеспечения системы управления рисками ПК-4.И-3. З-1 Знает современные принципы, методы и технологии работы с информацией ПК-4.И-3. З-2 Знает принципы и методы управления проектами ПК-4.И-3. З-3 Знает положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности ПК-4.И-4. З-1 Знает различные информационные ресурсы и технологии, про-

				ности ПК-4.И-4 Применяет в профессиональной деятельности современные информационные технологии, используемые в сфере управления рисками, работает с различными информационными ресурсами и технологиями, использует программные обеспечения для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных) на уровне опытного пользователя ПК-4. И-5 Использует в профессиональной деятельности основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации, компьютерную технику, оснащенную альтернативными устройствами ввода-вывода информации, адаптивные технические средства для людей с ограниченными возможностями здоровья	и методы управления проектами, ПК-4.И-3. У-3 Умеет использовать положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности ПК-4.И-4. У-1 Умеет применять в профессиональной деятельности современные информационные технологии, используемые в сфере управления рисками; ПК-4.И-4. У-2 Умеет работать с различными информационными ресурсами и технологиями, программными обеспечениями для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных) на уровне опытного пользователя. ПК-4. И-5. У-1 Умеет использовать в профессиональной деятельности основные методы, способы и средства получения, хранения, поиска, систематиза-	граммные обеспечения для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных) ПК-4. И-5. З-1 Знает основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации, ПК-4. И-5. З-2 Знает принципы работы с компьютерной техникой, оснащенной альтернативными устройствами ввода-вывода информации, адаптивными техническими средствами для людей с ограниченными возможностями здоровья ПК-4. И-6. З-1 Знает принципы и требования обеспечения сохранения государственной и коммерческой тайны и конфиденциальной информации; ПК-4. И-6. З-2 Знает принципы работы в системах электронного документо-

				ПК-4. И-6 Решает поставленные задачи в области системных и прикладных вопросов защиты информации в системах электронного документооборота на основе действующего российского законодательства с помощью современных принципов, методов и средств в различных организационных структурах, по базовым направлениям защиты государственной и коммерческой тайны и конфиденциальной информации	ции, обработки и передачи информации, компьютерную технику, оснащенную альтернативными устройствами ввода-вывода информации, адаптивные технические средства для людей с ограниченными возможностями здоровья ПК-4. И-6. У-1 Умеет решать поставленные задачи в области системных и прикладных вопросов защиты информации в системах электронного документооборота на основе действующего российского законодательства с помощью современных принципов, методов и средств в различных организационных структурах, по базовым направлениям защиты государственной и коммерческой тайны и конфиденциальной информации	оборота; ПК-4. И-6. З-3 Знает действующее российское законодательство в сфере защиты государственной и коммерческой тайны и конфиденциальной информации

2.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Инструменты, оценивающие сформированность компетенции	***Этапы и показатель оценивания компетенции***	***Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания***
УК-1; ОПК-7; ПК-4	*Тест*	*А) полностью сформирована (компетенция освоена на высоком уровне) – 90% правильных ответов* *Б) частично сформирована:* • *компетенция освоена на продвинутом уровне – 70% правильных ответов;* • *компетенция освоена на базовом уровне – от 51% правильных ответов;* *В) не сформирована (компетенция не сформирована) – менее 50% правильных ответов*	*Например:* *Проводится письменно. Время, отведенное на процедуру - 30 минут.* *Неявка – 0 баллов.* *Критерии оценки определяются процентным соотношением.* *Неудовлетворительно – менее 50% правильных ответов.* *Удовлетворительно - от 51% правильных ответов.* *Хорошо - от 70%.* *Отлично – от 90%.* *Максимальная оценка – 5 баллов.*
УК-1; ОПК-7; ПК-4	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	***Проводится в письменной и/или устной форме.*** ***Критерии оценки:*** ***1. Соответствие содержания доклада заявленной тематике (1 балл).*** ***2. Качество источников и их количество при подготовке работы (1 балл).*** ***3. Владение информацией и способность отвечать на вопросы аудитории (1 балл).*** ***4. Качество самой представленной работы (1 балл).*** ***5. Оригинальность подхода и всестороннее раскрытие выбранной тематики (1***

			балл). ***Максимальная сумма баллов - 5 баллов.***
УК-1; ОПК-7; ПК-4	***Выполнение контрольной работы***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов***	***При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида***

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерная тематика докладов в презентационной форме:

1. Информационная безопасность системы «Клиент – банк» на основе технологии «толстого клиента»
2. Информационная безопасность модели Интернет - банкинга.
3. Информационная безопасность расчетов банковскими картами в Интернете.
4. Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.
5. Схема защищенного информационного обмена при использовании симметричных методов защиты информации.
6. Схема защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.
7. Применение и информационная безопасность режима электронной кодовой книги. Режима сцепления блоков шифротекста. Режима обратной связи по шифротексту.

8. Режим счетчика (counter). Функция хеширования и асиметричные алгоритмы.

9. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET.

10. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).

11. Информационная безопасность при составление и направление ЭД участником – отправителем.

12. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.

13. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

Примерная тематика заданий на контрольную работу:

1. Информационная безопасность модели Интернет - банкинга.

2. Информационная безопасность расчетов банковскими картами в Интернете.

3. Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.

4. Схема защищенного информационного обмена при использовании симметричных методов защиты информации.

5. Схема защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.

6. Применение и информационная безопасность режима электронной кодовой книги. Режима сцепления блоков шифротекста. Режима обратной связи по шифротексту.

7. Режим счетчика (counter). Функция хеширования и асиметричные алгоритмы.

8. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET.

9. Информационная безопасность электронных платежуй с помощью цифровых денег.

10. Информационная безопасность расчетной функции банков и ее автоматизации. Схема обработки платежного документа клиентами.

11. Информационная безопасность и ключевые принципы для системно – значимых платежных систем. Определение количества ресурсов, которые банк будет держать на своих корсчетах.

12. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).

13. Информационная безопасность при составление и направление ЭД участником – отправителем.

14. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.

15. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Защита информации от несанкционированного доступа» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета.

Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
тестирование	УК-1; ОПК-7; ПК-4	30 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка - Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.
тестирование	УК-1; ОПК-7; ПК-4	30 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.
Экзамен	УК-1; ОПК-7; ПК-4	3 вопроса	Экзамен проводится в письменной форме, путем ответа на вопросы. Время, отведенное на	Результаты предоставляются в день проведения экзамена	Критерии оценки: «**Отлично**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике;

			процедуру – 30 минут.		• работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание «У**довлетворительно**»: • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; «**Неудовлетворительно**»: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях;

					• не отвечает на вопросы.

Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся, согласно приказу «О внедрении новой балльно-рейтинговой системы контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся» № 01-04/428 от 25 сентября 2020 г.

4.1. Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один вариант ответа.

1. Предмет, цель и задачи криптографии.
2. История криптографии.
3. Краткие сведения о криптоанализе.
4. Простейшие шифры и их свойства.
5. Системы шифрования с открытыми ключами.
6. Виртуальные частные сети.
7. Электронные цифровые подписи (электронные подписи).
8. Основные подходы к реализации PKI.
9. Компоненты и сервисы инфраструктуры открытых ключей.
10. Архитектура и топология PKI.
11. Стандарты в области PKI 50.
12. Стандарты Internet X.509 PKI (PKIX).
13. Сертификаты открытых ключей X.509.
14. Списки аннулированных сертификатов. Атрибутные сертификаты.
15. Основные требования к политике PKI.
16. Политика применения сертификатов и регламент.
17. Краткая характеристика политики PKI.
18. Набор положений политики PKI.
19. Проблемы формирования политики PKI.
20. Симметричные криптосистемы.
21. Основы теории К. Шеннона.
22. Симметричные методы шифрования.
23. Алгоритмы блочного шифрования.
24. Асимметричные системы шифрования.
25. Применение асимметричных алгоритмов.
26. Хранилище сертификатов ОС MS Windows.

Тестовые задания для контроля остаточных знаний

Вариант № 1

1. Как называется наука о способах преобразования информации с целью ее защиты от незаконных пользователей?
- Криптология
- Криптография
- Криптостойкость
- Криптометодология

2. Криптология включает в себя:
- Криптоанализ
- Криптография
- Криптосервис
- Криптостойкость

3. Системы шифрования, в которых для шифрования и для расшифрования используется один и тот же ключ относятся к:
- симметричным системам шифрования
- асимметричным системам шифрования
- одноключевым системам шифрования
- ключным системам

4. Простейшим из шифров замены является:
- одноалфавитная подстановка
- многоалфавитная замена
- гомофонический шифр
- малоалфавитная замена

5. Сколько этапов можно условно выделить в истории криптографии?
- 4
- 3
- 40
- 7

6. Для наивной криптографии (до начала XVI в.) характерно использование:
- любых, обычно примитивных, способов запутывания противника относительно содержания шифруемых текстов
- формализованных и относительно стойких к ручному криптоанализу шифров
- криптосистем со строгим математическим обоснованием криптостойкости
- вычислительных средств с производительностью, достаточной для реализации криптосистем, обеспечивающих при большой скорости шифрования на несколько порядков более высокую криптостойкость, чем "ручные" и "механические" шифры

7. Когда возникла компьютерная криптография?
- с 1970-х гг.
- с 1980-х гг.
- с 1990-х гг.
- с 2000-х гг.

8. В системе передачи данных между абонентами с коммутацией пакетов используются два способа передачи:
- дейтаграммный
- виртуальный
- параллельный
- перпендикулярный

9. Сколько уровней в эталонной модели OSI?
- 1
- 13
- 10
- 7

10. В каком году приняты определяющие нормативные правовые акты Российской Федерации: Концепция национальной безопасности Российской Федерации и Доктрина информационной безопасности Российской Федерации?
- 2000
- 1967
- 1998
- 2008

11. Подлежит ли деятельность по распространению шифровальных (криптографических) средств обязательному лицензированию?
- да
- нет
- для государственных учреждений нет, а для коммерческих предприятий да
- только для иностранных компаний, действующих на территории России

12. Какой уровень модели OSI обеспечивает создание, передачу и прием кадров данных? (Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов)
- канальный
- представления
- прикладной
- сеансовый

13. В каком ГОСТ-е дано определение термину "служебная тайна"?
- ГОСТ Р 51624-2000 “Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования”
- ГОСТ Р 51583-2000 “Защита информации. Порядок создания автоматизиро-

ванных систем в защищённом исполнении. Общие положения”
- ГОСТ Р ИСО\МЭК 15408
- Common Criteria

14. В Доктрине информационной безопасности РФ важное значение придано системам и сетям России, в том числе по следующим направлениям:
- предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств
- предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи
- предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации
- развитию свободы слова в Интернете

15. Основными мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

- закрытие всех интернет-кафе
- лицензирование деятельности организаций в области защиты информации
- сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите

Вариант № 2

1. Как называется наука о способах преобразования информации с целью ее защиты от незаконных пользователей?
- Криптология
- Криптография
- Криптостойкость
- Криптометодология

2. Криптология включает в себя:
- Криптоанализ
- Криптография
- Криптосервис
- Криптостойкость

3. Системы шифрования, в которых для шифрования и для расшифрования используется один и тот же ключ относятся к:
- симметричным системам шифрования
- асимметричным системам шифрования

•одноключевым системам шифрования
•ключным системам

4. Простейшим из шифров замены является:
•одноалфавитная подстановка
•многоалфавитная замена
•гомофонический шифр
•малоалфавитная замена

5. Сколько этапов можно условно выделить в истории криптографии?
•4
•3
•40
•7

6. Для наивной криптографии (до начала XVI в.) характерно использование:
•любых, обычно примитивных, способов запутывания противника относительно содержания шифруемых текстов
•формализованных и относительно стойких к ручному криптоанализу шифров
•криптосистем со строгим математическим обоснованием криптостойкости
•вычислительных средств с производительностью, достаточной для реализации криптосистем, обеспечивающих при большой скорости шифрования на несколько порядков более высокую криптостойкость, чем "ручные" и "механические" шифры

7. Когда возникла компьютерная криптография?
•с 1970-х гг.
•с 1980-х гг.
•с 1990-х гг.
•с 2000-х гг.

8. В системе передачи данных между абонентами с коммутацией пакетов используются два способа передачи:
•дейтаграммный
•виртуальный
•параллельный
•перпендикулярный

9. Сколько уровней в эталонной модели OSI?
•1
•13
•10
•7

10. В каком году приняты определяющие нормативные правовые акты Российской Федерации: Концепция национальной безопасности Российской Федерации

и Доктрина информационной безопасности Российской Федерации?

- 2000
- 1967
- 1998
- 2008

11. Подлежит ли деятельность по распространению шифровальных (криптографических) средств обязательному лицензированию?

- да
- нет
- для государственных учреждений нет, а для коммерческих предприятий да
- только для иностранных компаний, действующих на территории России

12. Какой уровень модели OSI обеспечивает создание, передачу и прием кадров данных? (Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов)

- канальный
- представления
- прикладной
- сеансовый

13. В каком ГОСТ-е дано определение термину "служебная тайна"?

- ГОСТ Р 51624-2000 “Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования”
- ГОСТ Р 51583-2000 “Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения”
- ГОСТ Р ИСО\МЭК 15408
- Common Criteria

14. В Доктрине информационной безопасности РФ важное значение придано системам и сетям России, в том числе по следующим направлениям:

- предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств
- предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи
- предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации
- развитию свободы слова в Интернете

15. Основными мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

- закрытие всех интернет-кафе
- лицензирование деятельности организаций в области защиты информации
- сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим ка-

налам систем и средств информатизации и связи

•введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите

Вариант № 3

1. Как называется наука о способах преобразования информации с целью ее защиты от незаконных пользователей?

•Криптология
•Криптография
•Криптостойкость
•Криптометодология

2. Криптология включает в себя:

•Криптоанализ
•Криптография
•Криптосервис
•Криптостойкость

3. Системы шифрования, в которых для шифрования и для расшифрования используется один и тот же ключ относятся к:

•симметричным системам шифрования
•асимметричным системам шифрования
•одноключевым системам шифрования
•ключным системам

4. Простейшим из шифров замены является:

•одноалфавитная подстановка
•многоалфавитная замена
•гомофонический шифр
•малоалфавитная замена

5. Сколько этапов можно условно выделить в истории криптографии?

•4
•3
•40
•7

6. Для наивной криптографии (до начала XVI в.) характерно использование:

•любых, обычно примитивных, способов запутывания противника относительно содержания шифруемых текстов
•формализованных и относительно стойких к ручному криптоанализу шифров
•криптосистем со строгим математическим обоснованием криптостойкости
•вычислительных средств с производительностью, достаточной для реализа-

ции криптосистем, обеспечивающих при большой скорости шифрования на несколько порядков более высокую криптостойкость, чем "ручные" и "механические" шифры

7. Когда возникла компьютерная криптография?
- с 1970-х гг.
- с 1980-х гг.
- с 1990-х гг.
- с 2000-х гг.

8. В системе передачи данных между абонентами с коммутацией пакетов используются два способа передачи:
- дейтаграммный
- виртуальный
- параллельный
- перпендикулярный

9. Сколько уровней в эталонной модели OSI?
- 1
- 13
- 10
- 7

10. В каком году приняты определяющие нормативные правовые акты Российской Федерации: Концепция национальной безопасности Российской Федерации и Доктрина информационной безопасности Российской Федерации?
- 2000
- 1967
- 1998
- 2008

11. Подлежит ли деятельность по распространению шифровальных (криптографических) средств обязательному лицензированию?
- да
- нет
- для государственных учреждений нет, а для коммерческих предприятий да
- только для иностранных компаний, действующих на территории России

12. Какой уровень модели OSI обеспечивает создание, передачу и прием кадров данных? (Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов)
- канальный
- представления
- прикладной
- сеансовый

13. В каком ГОСТ-е дано определение термину "служебная тайна"?

- ГОСТ Р 51624-2000 “Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования”
- ГОСТ Р 51583-2000 “Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения”
- ГОСТ Р ИСО\МЭК 15408
- Common Criteria

14. В Доктрине информационной безопасности РФ важное значение придано системам и сетям России, в том числе по следующим направлениям:

- предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств
- предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи
- предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации
- развитию свободы слова в Интернете

15. Основными мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

- закрытие всех интернет-кафе
- лицензирование деятельности организаций в области защиты информации
- сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите

4.2.Типовые вопросы, выносимые на экзамен

1. Предмет, цель и задачи криптографии.
2. История криптографии.
3. Краткие сведения о криптоанализе.
4. Классификация методов криптографического закрытия информации
5. Классические шифры.
6. Шифры гаммирования и колонной замены.
7. Простейшие шифры и их свойства.
8. Композиции шифров.
9. Системы шифрования с открытыми ключами.
10. Криптографическая стойкость шифров.
11. Модели шифров.
12. Основные требования к шифрам.
13. Вопросы практической стойкости.
14. Имитостойкость и помехоустойчивость шифров.
15. Принципы построения криптографических алгоритмов

16. Аппаратные средства. Программные средства, программные реализации шифров.
17. Крипто сервис провайдеры (CSP).
18. Особенности использования вычислительной техники в криптографии вопросы организации сетей засекреченной связи; ключевые системы.
19. Виртуальные частные сети.
20. Скремблеры.
21. Криптографические параметры узлов и блоков шифраторов.
22. Синтез шифров.
23. Методы получения случайных и псевдослучайных последовательностей.
24. Электронные цифровые подписи (электронные подписи).
25. Криптографические хеш-функции.
26. Криптографические протоколы.
27. Основные подходы к реализации PKI.
28. Компоненты и сервисы инфраструктуры открытых ключей.
29. Архитектура и топология PKI.
30. Стандарты в области PKI 50.
31. Стандарты Internet X.509 PKI (PKIX).
32. Сертификаты открытых ключей X.509.
33. Списки аннулированных сертификатов. Атрибутные сертификаты.
34. Основные требования к политике PKI.
35. Политика применения сертификатов и регламент.
36. Краткая характеристика политики PKI.
37. Набор положений политики PKI.
38. Проблемы формирования политики PKI.
39. Симметричные криптосистемы.
40. Основы теории К. Шеннона.
41. Симметричные методы шифрования.
42. Алгоритмы блочного шифрования.
43. Режимы применения блочных шифров.
44. Потоковые шифры.
45. Комбинированные методы.
46. Односторонние функции и функции ловушки.
47. Асимметричные системы шифрования.
48. Применение асимметричных алгоритмов.
49. Средства криптографической защиты, разработанные компаниями: Инфотекс, Крипто-Про, ОКБ Сапр, Аладдин и Adobe, MS Windows, Cisco.
50. Хранилище сертификатов ОС MS Windows.

Приложение 2

Методические указания для обучающихся по освоению дисциплины (модуля)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

«ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ»

Специальность: 38.05.01 Экономическая безопасность

Специализация: Экономико-правовое обеспечение экономической безопасности

Квалификация (степень) выпускника: экономист

Форма обучения: очная, заочная

Королев
2023

1. Общие положения

Цель дисциплины:

- формирование у студентов специализированной базы знаний по основным понятиям в области системных и прикладных вопросов защиты конфиденциальной информации;
- усовершенствовать навыки по основам практического обоснования требований к системе защиты конфиденциальной информации, что позволит студенту ориентироваться на рынке средств информационной защиты при выборе оптимального решения.

Задачи дисциплины:

- научить студентов самостоятельно решать поставленные задачи в области системных и прикладных вопросов защиты информации на основе действующего российского законодательства с помощью современных принципов, методов, сил и средств в различных организационных структурах, по базовым направлениям защиты государственной тайны и конфиденциальной информации;
- формирование у обучающихся правовой системы знаний, умений и навыков по защите информации;
- обеспечению информационной безопасности граждан, общества и государства, в частности раскрытие общих положений по защите информации;
- научить студентов самостоятельно решать поставленные задачи в области защищенности конфиденциальной информации с применением систем и средств защиты информации;
- ознакомить студентов с перспективными технологиями и методами защиты информации;
- изучить современные методики применения и использования встроенных механизмов защиты информации;
- научить студентов, порядку применения технических средств защиты информации.

2. Указания по проведению практических занятий

Раздел 1. Обеспечение безопасного допуска к информационным ресурсам

Тема 1. Технология контроля санкционированных событий. Парольная аутентификация

Практическое занятие 1.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Основные положения темы занятия:

- базовые составляющие концепции информационной безопасности информационного объекта.
- основные направления обеспечения информационной безопасности.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Конфиденциальность. Целостность. Подлинность. Неотрекаемость (невозможность отказа). Доступность. Анонимность.
2. Фундаментальные угрозы – утечка информации, нарушение целостности, отказ в обслуживании, незаконное использование. Первичные угрозы – проникновение (маскарад, обход защиты, нарушение полномочий) и внедрение (троянские программы, потайные ходы).
3. Шифрование. Цифровая подпись. Хэш-функция. Взаимосвязь услуг безопасности, механизмов и алгоритмов.

Продолжительность занятия:8/2 часов

Тема 2. Аутентификация с помощью биометрических характеристик

Практическое занятие 2.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных криптографических методов защиты информации.

Основные положения темы занятия:

- базовые составляющие криптографической защиты информации.
- криптосистемы и блочные шифры.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Базовая модель (отправитель ↔ злоумышленник ↔ получатель). Терминология: секретный/общедоступный ключи, открытый текст, шифртекст, криптоалгоритм, шифр, криптосистема, атака. Одноключевая (симметричная) криптосистема. Двухключевая (асимметричная) криптосистема или криптосистема с общедоступным ключом. Прямое криптографическое преобразование (зашифрование). Обратное криптографическое преобразование (расшифрование). Вычисление и проверка цифровой подписи. Код аутентичности сообщения (MAC). Метод цифрового конверта. Пассивные и активные атаки. Классификация атак.

2. Определение блочного шифра. Принцип итерирования. Конструкция Фейстеля. Режимы шифрования. (ECB, CBC, CFB, OFB, PCBC). Стандарты блочного шифрования – AES, ГОСТ-28147-89. Поточные шифры (на примере RC4). Схема одноразовых паролей (OTP). Минимальная длина ключа симметричной криптосистемы. Экспортные ограничения на длину ключа. Метод расширения ключевого пространства. Принцип несепарабельного шифрования. Многоуровневая криптография.

3. Криптосистема RSA. Практическая криптостойкость RSA: оценки и прогнозы. Криптосистема ЭльГамаля. Протокол согласования ключа Диффи-Хэллмана. Свойства цифровой подписи (подлинность, целостность, неотрекаемость). Федеральные стандарты цифровой подписи – DSS, ГОСТ Р 34.10 2001 (группа точек эллиптической кривой).

4. Свойства хэш-функци. Функция сжатия, как основной метод построения хэш-функций. Ключевые и бесключевые хэш-функции. Алгоритм HMAC. Федеральные стандарты хэш-функций – SHS, ГОСТ Р 34.11-94. MD5 – de facto стандарт Internet. Парадокс «дней рождения». Атаки на основе парадокса «дней рождения».

Продолжительность занятия:8/2 часов

Раздел 2. Учет субъектов доступа. Реализация механизмов защиты

Тема 3. Практическая реализация механизмов добавочной защиты

Практическое занятие 3.

Вид практического занятия**: *подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных криптографических протоколов защиты информации.

Основные положения темы занятия:

- базовые протоколы криптографической защиты информации.
- квантовая криптография.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Принципы проектирования криптографических протоколов по Нидхему-Шредеру. Протокол «запрос-ответ».

2. Анонимность и неотслеживаемость. Проблема «ужинающих криптографов». Протоколы для анонимных чеков на основе «слепой» подписи. Свойства идеальной системы электронных наличных. Платежных систем Payword и Micromint.

3. Протокол электронного аукциона, отвечающий требованиям Федерального Закона № 94 от 21 июля 2005 года «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд».

4. Принципы квантовой криптографии. Квантовый протокол распределения ключей.

5. Обзор биометрических методов. Метод биометрической «вуали».

Продолжительность занятия:8/2 часов

Тема 4. Разработка и оптимизация механизма уровневого контроля, как механизма реального времени
Практическое занятие 4.

Вид практического занятия**: *подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки управления ключами.

Основные положения темы занятия:

- Управление ключами.
- Взаимодействие с УЦ.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Генерация ключей. Неравносильные ключи. Распределение. Проверка. Использование. Обновление. Хранение и резервирование. Уничтожение. Жизненный цикл ключа. пределения ключей Baffine.
2. Метод полной матрицы. Проблема «квадратного корня». Облегченная схема предварительного распределения ключей KEDYS. Облегченная схема предварительного распределения ключей для кластерной архитектуры EKSYD. Проблема подлинности открытых ключей – на примере атаки «человек посередине» (man-in-the-middle-attack). Цифровой сертификат (по Конфелдеру).
3. Сертификат, подписчик, пользователь, выпуск сертификата, аннулирование открытого ключа, отзыв сертификата, список отозванных сертификатов (СОС), приостановление действия сертификата, Удостоверяющий Центр (УЦ), Центр регистрации (ЦР), взаимная (перекрестная) сертификация. Жизненный цикл сертификата. Архитектура PKI. Понятие сертификационного пути. Преимущества PKI.
4. Непосредственный контакт. Удаленный доступ. Разделение функциональности. Расширение функциональности.

Продолжительность занятия: 8/2 часов

4. Указания по проведению самостоятельной работы студентов

Цель самостоятельной работы: подготовить студентов к самостоятельному научному творчеству.

Задачи самостоятельной работы:

1) расширить представление в области существующих современных аппаратных средств вычислительной техники;

2) привить навыки самостоятельного решения нестандартных задач в области аппаратных средств вычислительной техники.

Объем времени на самостоятельную работу, и виды самостоятельной работы представлены в таблице 1.

Таблица 1

Объем времени и виды самостоятельной работы

Виды самостоятельной работы	**Очная форма обучения/заочная форма обучения**
	Всего академических часов
Всего часов на самостоятельную работу	60/92
Вопросы, выносимые на самостоятельное изучение	15/22
Подготовка к практическим занятиям	15/22
Подготовка к лабораторным занятиям	нет
Подготовка докладов	15/24
Выполнение практических заданий	15/24

Вопросы, выносимые на самостоятельное изучение:

для очной формы обучения:

1. Информационная безопасность системы «Клиент – банк» на основе технологии «толстого клиента»
2. Информационная безопасность модели Интернет - банкинга.
3. Информационная безопасность расчетов банковскими картами в Интернете.
4. Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.
5. Схема защищенного информационного обмена при использовании симметричных методов защиты информации.
6. Схема защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.
7. Применение и информационная безопасность режима электронной кодовой книги. Режима сцепления блоков шифротекста. Режима обратной связи по шифротексту.
8. Режим счетчика (counter). Функция хеширования и ассиметричные алгоритмы.
9. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET.
10. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).

11. Информационная безопасность при составление и направление ЭД участником – отправителем.

12. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.

13. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

для заочной формы обучения:

1. Информационная безопасность системы «Клиент – банк» на основе технологии «толстого клиента»
2. Информационная безопасность модели Интернет - банкинга.
3. Информационная безопасность расчетов банковскими картами в Интернете.
4. Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.
5. Схема защищенного информационного обмена при использовании симметричных методов защиты информации.
6. Схема защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.
7. Применение и информационная безопасность режима электронной кодовой книги. Режима сцепления блоков шифротекста. Режима обратной связи по шифротексту.
8. Режим счетчика (counter). Функция хеширования и ассиметричные алгоритмы.
9. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET.
10. Информационная безопасность электронных платежей с помощью цифровых денег.
11. Информационная безопасность расчетной функции банков и ее автоматизации. Схема обработки платежного документа клиентами.
12. Информационная безопасность и ключевые принципы для системно – значимых платежных систем. Определение количества ресурсов, которые банк будет держать на своих корсчетах.
13. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).
14. Информационная безопасность при составлении и направление ЭД участником – отправителем.
15. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.
16. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

Тематическое содержание самостоятельной работы представлено в таблице

2.

Таблица 2

Тематическое содержание самостоятельной работы

№ п/п	Виды самостоятельной работы	Количество часов	Перечень заданий
1.	Вопросы, выносимые на самостоятельное изучение	15/22	Изучение открытых источников
2.	Подготовка к практическим занятиям	15/22	Изучение открытых источников при подготовке доклада на выбранную тему.
3.	Подготовка к лабораторным занятиям	нет	Изучение открытых источников
4.	Тематика докладов	15/24	1. Внутренние аппаратные средства персонального компьютера 2. Внешние периферийные устройства персонального компьютера
5.	Выполнение практических заданий	15/24	Разработка аппаратного средства вычислительной техники по заданным характеристикам

Примерные темы докладов

1. Предмет, цель и задачи криптографии.
2. История криптографии.
3. Краткие сведения о криптоанализе.
4. Простейшие шифры и их свойства.
5. Системы шифрования с открытыми ключами.
6. Виртуальные частные сети.
7. Электронные цифровые подписи (электронные подписи).
8. Основные подходы к реализации PKI.
9. Компоненты и сервисы инфраструктуры открытых ключей.
10. Архитектура и топология PKI.
11. Стандарты в области PKI 50.
12. Стандарты Internet X.509 PKI (PKIX).
13. Сертификаты открытых ключей X.509.
14. Списки аннулированных сертификатов. Атрибутные сертификаты.
15. Основные требования к политике PKI.
16. Политика применения сертификатов и регламент.
17. Краткая характеристика политики PKI.
18. Набор положений политики PKI.
19. Проблемы формирования политики PKI.
20. Симметричные криптосистемы.
21. Основы теории К. Шеннона.

22. Симметричные методы шифрования.
23. Алгоритмы блочного шифрования.
24. Асимметричные системы шифрования.
25. Применение асимметричных алгоритмов.
26. Хранилище сертификатов ОС MS Windows.

5. Указания по проведению контрольных работ

5.1. Требования к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.
2. Основная часть работы раскрывает процесс проектирования заданного аппаратного устройства и должна содержать соответствующие таблицы или временные диаграммы, которые должны формироваться разрабатываемым устройством, принципиальную схему устройства и описание его работы.
3. В процессе изложения материала необходимо давать ссылки на используемую литературу.
4. Заключение должно содержать сделанные автором работы выводы, итоги исследования.
5. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями.

5.3. Требования к оформлению

Объём контрольной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

Рекомендуемая тематика

1. Сущность и понятие информационной безопасности
2. Значение информационной безопасности и ее место в системе национальной безопасности. Доктрина информационной безопасности РФ
3. Сущность и теоретико-концептуальные основы защиты информации
4. Характеристика защищаемой информации
5. Критерии, условия и принципы отнесения информации к защищаемой.
6. Состав и классификация ЗИ и их носителей
7. Основы защиты коммерческой тайны
8. Основы защиты государственной тайны
9. Основы защиты личной тайны
10. Основы защиты профессиональной тайны
11. Условия, определяющие необходимость защиты информации
12. Дестабилизирующие воздействия на защищаемый информационный ресурс.
13. Каналы противоправных действий в информационной безопасности
14. Методы противоправных действий в информационной безопасности

15. Характеристика деятельности разведывательных служб по несанкционированному доступу к защищаемому информационному ресурсу 16. Общая характеристика основных мер по защите информации (информационной безопасности)

17. Основные виды обеспечение, системы и средства защиты информации (информационной безопасности)

18. Основные виды обеспечение защиты информации (информационной безопасности)

19. Основные виды системы защиты информации (информационной безопасности)

20. Классификация средств защиты информации (информационной безопасности)

21. Основы управления информационной безопасности

22. Основы оценки эффективности защиты информации

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ИНФРА-М, 2022. — 256 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016535-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1861659 (дата обращения: 03.10.2022). – Режим доступа: по подписке.

2. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. - Новосибирск : Изд-во НГТУ, 2019. - 83 с. - ISBN 978-5-7782-3918-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1866895 (дата обращения: 03.10.2022). – Режим доступа: по подписке.

Дополнительная литература:

3. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: https://doi.org/10.29039/01848-4. - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232287 (дата обращения: 03.10.2022). – Режим доступа: по подписке.

4. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: 60x90 1/16. - (Высшее образование: Бакалавриат; Магистратура). (переплет) ISBN 978-5-369-01378-6http://znanium.com/bookread2.php?book=474838

5. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429070

6. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2016 - 120 с.: 60x88 1/16 + (Доп. мат. znanium.com). - (Высшее образование: Бакалавр.). (о) ISBN 978-5-369-01379-3http://znanium.com/bookread2.php?book=549914

7. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие / Наталия Васильевна. – 2 ; доп. – М.: Издательство «ФОРУМ» : ООО «Научно-издательский центр ИНФРА-М», 2016. – 240 с. – ISBN 978-5-00091-007-8. URL: http://znanium.com/go.php?id=544554

8. Загинайлов, Ю. Н. Основы информационной безопасности : курс визуальных лекций / Ю. Н. Загинайлов ; Ю.Н. Загинайлов. - М. |Берлин : Директ-Медиа, 2015. - 105 с. - ISBN 978-5-4475-3947-4. URL: http://biblioclub.ru/index.php?page=book&id=362895

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp** – научно-образовательный портал.
2. **http://informika.ru/** – образовательный портал.
3. **www.wikIsec.ru** - Энциклопедия информационной безопасности. – Публикации, статьи.
4. **www.biblioclub.ru** - Универсальная библиотека онлайн.
5. **www.rucont.ru** - ЭБС «Руконт».
6. **http://www.academy.it.ru/** - академия АЙТИ.
7. **http://www.minfin.ru/** - Официальный сайт Министерства финансов Российской Федерации
8. **http://www.gov.ru/** - Официальный сервер органов государственной власти Российской Федерации.
9. **http://www.fsb.ru/** - Официальный сайт Федеральной Службы Безопасности
10. **http://www.fstec.ru/** - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

8. Перечень информационных технологий

Перечень программного обеспечения: *MSOffice, Multisim.*

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды Университет
2. Рабочая программа и методическое обеспечение по дисциплине «Защита конфиденциальной информации».