

МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

«Утверждаю»
Заведующий кафедрой ТО и ЗИ



А.А. Сирота
«22» 12 2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.03 Технологии защищенного документооборота и блокчейн

1. Код и наименование направления подготовки / специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки / специализация/магистерская программа:

Разработка защищенного программного обеспечения

3. Квалификация (степень) выпускника:

Специалист

4. Форма обучения:

Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра технологий обработки и защиты информации

6. Составители программы:

Вялых Сергей Ариевич, кандидат технических наук

7. Рекомендована:

протокол НМС ФКН № 3 от 22.11.2023 г.

8. Учебный год: 2027-2028

Семестр(ы): 8

9. Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

Изучение теоретических основ и овладение практическими навыками применения методов и средств электронной подписи, технологий блокчейн для организации защищенного документооборота, в интересах обеспечения мер защиты информации при разработке, сопровождении и проектировании информационных систем различного назначения; получение профессиональных компетенций в области современных технологий обработки и защиты информации.

Задачи дисциплины:

- обучение студентов базовым понятиям современных технологий обработки информации с использованием электронной подписи;
- освоение студентами положений и требований, современных нормативно-методических документов, регламентирующих использование электронной подписи;
- освоение студентами положений инфраструктуры открытых ключей (англ. PKI - Public Key Infrastructure) для поддержки криптозадач на основе закрытого и открытого ключей;
- освоение технологии формирования квалифицированных сертификатов ключей проверки электронной подписи и освоение практических решений применения технологий защищённого документооборота;
- овладение практическими навыками применения алгоритмов обработки информации с использованием электронной подписи;
- формирование представления об угрозах безопасности информации при использовании электронной подписи и основных требованиях к удостоверяющим центрам, средствам электронной подписи и квалифицированным сертификатам проверки электронной подписи;
- овладение практическими навыками применения алгоритмов обработки информации с использованием электронной подписи;
- формирование представления о технологиях блокчейн.

10. Место учебной дисциплины в структуре ООП:

Входит в часть, формируемую участниками образовательных отношений (вариативная) блока Б1.

Для успешного освоения дисциплины необходимы входные знания в области криптографических методов защиты информации, систем подготовки электронных документов, инструментальных средств информационных систем, администрирования и управления безопасностью интранет-сетей и сетевых технологий.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ПК-1	Способен проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения	ПК-1.2	Знает применяемые математические методы и алгоритмы функционирования для компонентов программных средств	Знать: программные компоненты и особенности реализации электронной подписи и средств криптозащиты информации Уметь: проводить анализ безопасности компьютерных систем, использующих средства электронной подписи Владеть: навыками построения и анализа безопасности информационных систем использующих электронную подпись
		ПК-1.3	Умеет применять технологии обработки данных, анализировать воз-	Знать: роль и особенности применения методов и средств криптозащиты информации в современных компьютерных системах Уметь: производить установку, наладку, тестирование и обслуживание современных

			<p>возможности их использования при разработке программного обеспечения в профессиональной деятельности</p>	<p>средств криптографической защиты информации</p> <p>Владеть: практическими навыками развертывания удостоверяющего центра для реализации технологий с использованием квалифицированной электронной подписи</p>
ПК-3	Способен проводить анализ безопасности программных средств в компьютерных системах	ПК-3.2	<p>Знает современные технологии защиты электронного документооборота, технологии защиты объектов электронного контента от несанкционированного использования</p>	<p>Знать: требования нормативных документов, методы анализа информационной безопасности при проектировании и эксплуатации информационных систем при использовании средств электронной подписи</p> <p>Уметь: анализировать и разрабатывать модели угроз для различных объектов защиты при использовании средств электронной подписи</p> <p>Владеть: практическими навыками формирования требований безопасности информации для различных классов и уровней защищенности информационных систем</p>
		ПК-3.4	<p>умеет анализировать возможности использования современных технологий защиты данных и объектов электронного контента</p>	<p>Знать: базовые понятия, требования нормативных документов, методы анализа информационной безопасности при проектировании и эксплуатации информационных систем при использовании средств электронной подписи</p> <p>Уметь: анализировать и разрабатывать модели угроз для различных вариантов построения защищенных информационных систем при использовании электронной подписи</p> <p>Владеть: практическими навыками формирования требований безопасности информации для различных классов и уровней защищенности информационных систем</p>

12. Объем дисциплины в зачетных единицах/час — 4/144.

Форма промежуточной аттестации: зачет.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			№ семестра 8	№ семестра	Итого
Аудиторные занятия		56	56		56
в том числе:	лекции	28	28		28
	практические	14	14		14
	лабораторные	14	14		14
Самостоятельная работа		88	88		88
в том числе: курсовая работа (проект)		-	-		-
Форма промежуточной аттестации (экзамен – _ час.)		-	-		-
Итого:		144	144		144

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК *
1. Лекции			Создан электронный онлайн - курс, размещены материалы к лекции и лабораторным работам
1.1	Инфраструктура открытых ключей и электронная подпись	<p>1. Электронная подпись, назначение и применение, история возникновения, используемые алгоритмы.</p> <p>2. Сертификат ключа проверки электронной подписи. Основные понятия и определения.</p> <p>3. Хранение закрытого ключа. Основные угрозы криптоатак.</p> <p>4. Инфраструктура открытых ключей (PKI). Удостоверяющий центр. Возможные архитектуры построения PKI.</p>	
1.2	Нормативно-правовые документы, регламентирующие применение электронной подписи	<p>5. Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи». Виды электронной подписи.</p> <p>6. Приказ Минкомсвязи России от 23.11.2011 N 320 "Об аккредитации удостоверяющих центров".</p> <p>7. Приказ ФСБ от 27 декабря 2011 г. N 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи». Приказ ФСБ от 27 декабря 2011 г. N 796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра».</p>	
1.3	Технологии формирования закрытых ключей и сертификатов открытых ключей проверки электронной подписи	<p>8. Криптопровайдеры. Основные технологии, используемые при развёртывании удостоверяющих центров.</p> <p>9. Развёртывание удостоверяющего центра КриптоПро УЦ. Основные задачи, выполняемые на удостоверяющем центре. Требования по безопасности информации.</p>	
1.4	Средства электронной подписи	<p>10. Типовые решения, реализующие возможность применения электронной подписи.</p> <p>11. Универсальная электронная карта. Портал государственных услуг Российской Федерации, электронная почта, текстовые редакторы, специализированные средства.</p>	
1.5	Угрозы безопасности информации и основные направления защиты, связанные с использованием электронной подписи	<p>12. Угрозы безопасности информации при использовании электронной подписи.</p> <p>13. Основные направления защиты, связанные с использованием электронной подписи.</p>	
1.6	Блокчейн. Основные понятия	<p>14. Архитектура программного обеспечения и ее связь с технологией блокчейна. Преимущества и недостатки распределенных систем. Реализация и поддержка целостности в распределенных системах.</p> <p>15. Обеспечение доверительности и целостности в распределенных системах. Право владения и блокчейн. Проблема двойного расходования.</p> <p>16. Примеры структур данных и алгоритмов, решающих задачи реализации блокчейн технологий.</p>	

1.7	Перспективы и практическое использование блокчейн технологий	17. Перспективы и практическое использование блокчейн технологий.	
2. Практические занятия			Создан электронный онлайн - курс, размещены материалы к лекции и лабораторным работам
2.1	Инфраструктура открытых ключей и электронная подпись	1. Изучение основных возможностей программных реализаций сертифицированных средств криптозащиты информации (КриптоПро CSP, VipNet CSP.).	
2.2	Нормативно-правовые документы, регламентирующие применение электронной подписи	2. Оценка типа и принятие решения о доверии электронной подписи. 3. Изучение возможностей программы Крипто-Арм.	
2.3	Технологии формирования закрытых ключей и сертификатов открытых ключей проверки электронной подписи	4. Изучение возможностей применения электронных носителей информации для работы с электронной подписью.	
2.4	Средства электронной подписи	5. Изучение типовых средств и способов применения и использования электронной подписи.	
3. Лабораторные работы			Создан электронный онлайн - курс, размещены материалы к лекции и лабораторным работам
3.1	Инфраструктура открытых ключей и электронная подпись	1. Исследование возможных вариантов применения и возможностей управления сертификатами в операционной системе Windows. 2. Сравнительный анализ возможностей типовых криптопровайдеров.	
3.2	Нормативно-правовые документы, регламентирующие применение электронной подписи	3. Исследование и оценка надежности алгоритмов установления доверия к электронной подписи.	
3.3	Технологии формирования закрытых ключей и сертификатов открытых ключей проверки электронной подписи	4. Развертывание удостоверяющего центра КриптоПро УЦ. 5. Исследование возможностей применения удостоверяющего центра для работы с электронной подписью	
3.4	Средства электронной подписи	6. Использование электронной подписи для защиты документооборота.	
3.5	Угрозы безопасности информации и основные направления защиты, связанные с использованием электронной подписи	7. Исследование возможностей извлечения и неправомерного использования закрытого ключа электронной подписи.	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)				
		Лекции	Лаб.	Прак.	Сам. работа	Всего
1	Инфраструктура открытых ключей и электронная подпись	6	4	4	12	26
2	Нормативно-правовые документы, регламентирующие применение электронной подписи	4	2	4	14	24
3	Технологии формирования закрытых ключей и сертификатов открытых ключей проверки электронной подписи	4	4	4	14	26
4	Средства электронной подписи	4	2	2	12	20

5	Угрозы безопасности информации и основные направления защиты, связанные с использованием электронной подписи	4	2	-	12	18
6	Блокчейн. Основные понятия	4	-	-	12	16
7	Практическое использование и перспективы блокчейн технологий	2	-	-	12	14
	Итого:	28	14	14	88	144

14. Методические указания для обучающихся по освоению дисциплины

(рекомендации обучающимся по освоению дисциплины: работа с конспектами лекций, презентационным материалом, выполнение практических заданий, тестов, заданий текущей аттестации и т.д.)

1) При изучении дисциплины рекомендуется использовать следующие средства:

- рекомендуемую основную и дополнительную литературу;
- методические указания и пособия;
- контрольные задания для закрепления теоретического материала;

электронные версии учебников и методических указаний для выполнения лабораторно-практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, решение задач) студентов по материалам лекций и практических работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала. Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

3) При проведении лабораторных занятий обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка методов, алгоритмов и технологий обработки информации, излагаемых в рамках лекций.

В ходе самостоятельной работы необходимо уделить основное внимание работе с текстом конспекта лекции, изучению рекомендованной литературы, изучению нормативных документов по информационной безопасности.

4) При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей, вовремя подключаться к online занятиям, ответственно подходить к заданиям для самостоятельной работы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)

а) основная литература:

№ п/п	Источник
1	Скудис, Эд. Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите : / Э. Скудис .— Москва : ДМК Пресс, 2009 .— 512 с. : ил. — (Защита и администрирование) .— .— ISBN 5-94074-170-3 : 176-00 .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1112>.

б) дополнительная литература:

№ п/п	Источник
2	Фостер, Джеймс. Защита от взлома: сокетты, эксплойты, shell-код : / Дж. Фостер, М. Прайс ; пер. с англ. А. А. Слинкина .— Москва : ДМК Пресс, 2008 .— 784 с. : ил. — (Информационная безопасность) .— .— ISBN 5-9706-0019-9 : 449.10 p. — <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1117>.
3	Ищейнов, Вячеслав Яковлевич. Защита конфиденциальной информации : [учебное пособие для студ. вузов., обуч. по специальности 090103 "Организация и технология защиты информации" и 090104 "Комплексная защита объектов информатизации"] / В.Я. Ищейнов, М.В. Мецатунян .— М. : ФОРУМ, 2009 .— 254 с. : ил. — (Высшее образование) .— Библиогр.: с.249-254 .— ISBN 978-5-91134-336-1.
4	Гражданский кодекс Российской Федерации, часть 1, глава 9, статья 160

5	ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи
6	Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи»
7	Антонопулос А.М. Осваиваем биткоин / пер. с англ. А.В. Снастина. – М.: ДМК Пресс, 2018. - 428 с.: ил. ISBN 978-5-94074-965-3
7	Основы блокчейна: вводный курс для начинающих в 25 небольших главах: ДМК Пресс; Москва; 2018 ISBN 978-5-97060-591-2
8	Технология блокчейн: то, что движет финансовой революцией сегодня / Дон Тапскотт, Алекс Тапскотт ; [пер. с англ. К. Шашковой, Е. Ряхиной]: Эксмо; Москва; 2017 ISBN 978-5-699-95092-8
9	Блокчейн: Как это работает и что ждет нас завтра / Артем Генкин, Алексей Михеев»: Альпина Паблшер; Москва; 2018 ISBN 978-5-9614-5046-0

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурс
10	Элементы теории чисел и криптозащита : учебное пособие для вузов. Ч. 2 / Воронеж. гос. ун-т; сост.: Б.Н. Воронков, А.С. Щеголеватых .— Воронеж : ИПЦ ВГУ, 2008 .— 95 с. : ил. — Библиогр.: с.95 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m08-238.pdf>
11	http://www.cryptopro.ru
12	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
13	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
14	ЭБС Лань, Лицензионный договор №3010, (с 01/03/2024 по 28.02.2025) 06/02 24 от 13.02.2024 (с дополнительным соглашением №1 от 14.03.2024), ЭБС «Университетская библиотека online» (Контракт №3010 06/11 23 от 26.12.2023 (с 26.12.2023 по 25.12.2024), ЭБС «Консультант студента» – Лицензионный договор №980КС/12-2023 / 3010-06/01-24 от 24.01.2024 с 24.01.2024 по 11. 01.2025), Электронная библиотека ВГУ, Договор №ДС-208 от 01.02.2021 с ООО «ЦКБ «БИБКОМ» и ООО «Агентство «Книга-Сервис» о создании Электронной библиотеки ВГУ, (с 01.02.2021 по 31.01.2027), ЭБС BOOK.ru, Договор №3010 15/983 23 от 20.12.2023, (с 01.02.2024 по 31.01.2025)

16. Перечень учебно-методического обеспечения для самостоятельной работы

(учебно-методические рекомендации, пособия, задачки, методические указания по выполнению практических (контрольных) работ и др.)

№ п/п	Источник
1	http://www.infotecs.ru
2	http://www.rsdn.ru/article/crypto/cspsecrets.xml Секреты разработки CSP для Windows. Создание криптографического провайдера для Windows. Зырянов Юрий Сергеевич, ООО "ЛИССИ". Источник: RSDN Magazine #3-2006
3	http://www.lissi-crypto.ru/
4	http://www.signal-com.ru
5	http://www.cryptopro.ru
6	http://www.shipka.ru
7	Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2024. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/537383 (дата обращения: 30.06.2024).

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ, электронное обучение (ЭО), смешанное обучение):

Для реализации учебного процесса используется установленная версия пакета среды виртуализации Oracle VM VirtualBox; образы операционных систем семейства Windows v.7, 8, 10, Windows Server v. 2008-2019; Microsoft SQL Server; доступ в сеть

Интернет; LibreOffice v.5-7; Foxit PDF Reader; Справочно-правовая система (СПС) Консультант+ для образования.

При реализации дисциплины могут использоваться технологии электронного обучения и дистанционные образовательные технологии на базе портала edu.vsu.ru, а также другие доступные ресурсы сети Интернет.

18. Материально-техническое обеспечение дисциплины:

1) Учебная аудитория (компьютерный класс) (одна из №1-4 корп. 1а, ауд. № 382-385): специализированная мебель, персональные компьютеры на базе i5-9600KF-3,7ГГц, мониторы ЖК 24” (16 шт.), специализированная мебель: доска маркерная 1 шт., столы 16 шт., стулья 33 шт.; доступ к фондам учебно-методической документации и электронным изданиям, доступ к электронным библиотечным системам, выход в Интернет. ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

2) Для проведения лабораторных и практических работ. Компьютерный класс (один из №1-3 корп. 1а, ауд. № 290, 293, 383), ПК-Intel-i7 16 шт. (с оперативной памятью не менее 8 гигабайт, рекомендуется 16 гигабайт), специализированная мебель: доска маркерная 1 шт., столы 16 шт., стулья 33 шт.; доступ к фондам учебно-методической документации и электронным изданиям, доступ к электронным библиотечным системам, выход в Интернет.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	1. Инфраструктура открытых ключей и электронная подпись 2. Нормативно-правовые документы, регламентирующие применение электронной подписи	ПК-1	ПКВ-1.2	Контрольная работа по соответствующим разделам. Лабораторная работа по соответствующим разделам.
2	3. Технологии формирования закрытых ключей и сертификатов открытых ключей проверки электронной подписи 4. Средства электронной подписи	ПК-1	ПК-1.3	Контрольная работа по соответствующим разделам. Лабораторная работа по соответствующим разделам.
3	5. Угрозы безопасности информации и основные направления защиты, связанные с использованием электронной подписи 6. Блокчейн. Основные понятия. 7. Перспективы и практическое использование блокчейн технологий	ПК-3	ПК-3.2 ПК-3.4	Контрольная работа по соответствующим разделам. Лабораторная работа по соответствующим разделам
Промежуточная аттестация форма контроля – зачет, КР				Перечень вопросов, практическое задание

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1. Текущий контроль успеваемости

Текущая аттестация проводится в соответствии с Положением о текущей аттестации

обучающихся по программам высшего образования Воронежского государственного университета.

Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная

беседа) и письменных работ (контрольные, лабораторные работы). При оценивании могут

использоваться количественные или качественные шкалы оценок.

Текущий контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных

средств:

Устный опрос; Контрольная работа по теоретической части курса; Лабораторные работы

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Контрольная работа по разделам дисциплины	Вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной в разделе 20.2
3	Лабораторная работа	Содержит 7 лабораторных заданий, предусматривающие разработку требований по уровням и классам защищенности различных информационных систем, разработки и внедрения их систем защиты, а также контроля ее эффективности.	При успешно выполнении работы ставится оценка зачтено и осуществляется допуск к экзамену, в противном случае ставится оценка не зачтено и обучающийся не допускается к экзамену.
4	КИМ промежуточной аттестации	Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает вопросы для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции.	Шкалы оценивания приведены в разделе 20.2

Приведённые ниже задания рекомендуется использовать при проведении диагностических работ для оценки остаточных знаний по дисциплине

Компетенция ПК-1

Задания закрытого типа

- 1. Указать в каких случаях (при использовании СКЗИ) для защиты персональных данных необходимо использовать СКЗИ класса КС1? Для нейтрализации атак, при создании способов, подготовке и проведении которых используются возможности:**
 - а) без привлечения специалистов в области разработки и анализа СКЗИ;
 - б) за пределами контролируемой зоны на данные, передаваемые по каналам связи;
 - в) при нахождении в пределах контролируемой зоны;
 - г) на этапе эксплуатации СКЗИ на следующие объекты: документацию на СКЗИ и компоненты среды функционирования;
 - д) физический доступ к средствам вычислительной техники, на которых реализованы СКЗИ и среда функционирования;
 - е) возможность располагать аппаратными компонентами СКЗИ и среды функционирования, ограниченными мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;
 - ж) с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и среду функционирования, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО;

з) проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

и) в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и среды функционирования, в том числе с использованием исходных текстов входящего в среду функционирования прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ;

к) создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО;

л) возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты среды функционирования;

м) возможность располагать всеми аппаратными компонентами СКЗИ и среды функционирования;

2. Указать в каких случаях (при использовании СКЗИ) для защиты персональных данных необходимо использовать средства криптозащиты информации (СКЗИ) класса КС2? Для нейтрализации атак, при создании способов, подготовке и проведении которых используются возможности:

а) без привлечения специалистов в области разработки и анализа СКЗИ;

б) за пределами контролируемой зоны на данные, передаваемые по каналам связи;

в) при нахождении в пределах контролируемой зоны;

г) на этапе эксплуатации СКЗИ на следующие объекты: документацию на СКЗИ и компоненты среды функционирования;

д) физический доступ к средствам вычислительной техники, на которых реализованы СКЗИ и среда функционирования;

е) возможность располагать аппаратными компонентами СКЗИ и среды функционирования, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

ж) с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и среду функционирования, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО;

з) проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

и) в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и среды функционирования, в том числе с использованием исходных текстов входящего в среду функционирования прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ;

к) создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО;

л) возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты среды функционирования;

м) возможность располагать всеми аппаратными компонентами СКЗИ и среды функционирования;

3. Указать в каких случаях (при использовании СКЗИ) для защиты персональных данных необходимо использовать средства криптозащиты информации (СКЗИ) класса КС3? Для нейтрализации атак, при создании способов, подготовке и проведении которых используются возможности:

а) без привлечения специалистов в области разработки и анализа СКЗИ;

б) за пределами контролируемой зоны на данные, передаваемые по каналам связи;

в) при нахождении в пределах контролируемой зоны;

г) на этапе эксплуатации СКЗИ на следующие объекты: документацию на СКЗИ и компоненты среды функционирования;

д) физический доступ к средствам вычислительной техники, на которых реализованы СКЗИ и среда функционирования;

е) возможность располагать аппаратными компонентами СКЗИ и среды функционирования, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

ж) с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и среду функционирования, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО;

з) проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

и) в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и среды функционирования, в том числе с использованием исходных текстов входящего в среду функционирования прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ;

к) создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО;

л) возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты среды функционирования;

м) возможность располагать всеми аппаратными компонентами СКЗИ и среды функционирования;

4. Указать в каких случаях (при использовании СКЗИ) для защиты персональных данных необходимо использовать средства криптозащиты информации (СКЗИ) класса КВ? Для нейтрализации атак, при создании способов, подготовке и проведении которых используются возможности:

а) без привлечения специалистов в области разработки и анализа СКЗИ;

б) за пределами контролируемой зоны на данные, передаваемые по каналам связи;

в) при нахождении в пределах контролируемой зоны;

г) на этапе эксплуатации СКЗИ на следующие объекты: документацию на СКЗИ и компоненты среды функционирования;

д) физический доступ к средствам вычислительной техники, на которых реализованы СКЗИ и среда функционирования;

е) возможность располагать аппаратными компонентами СКЗИ и среды функционирования, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

ж) с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и среду функционирования, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО;

з) проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

и) в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и среды функционирования, в том числе с использованием исходных текстов входящего в среду функционирования прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ;

к) создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО;

л) возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты среды функционирования;

м) возможность располагать всеми аппаратными компонентами СКЗИ и среды функционирования;

5. Указать в каких случаях (при использовании СКЗИ) для защиты персональных данных необходимо использовать средства криптозащиты информации (СКЗИ) класса КА? Для нейтрализации атак, при создании способов, подготовке и проведении которых используются возможности:

а) без привлечения специалистов в области разработки и анализа СКЗИ;

б) за пределами контролируемой зоны на данные, передаваемые по каналам связи;

в) при нахождении в пределах контролируемой зоны;

г) на этапе эксплуатации СКЗИ на следующие объекты: документацию на СКЗИ и компоненты среды функционирования;

д) физический доступ к средствам вычислительной техники, на которых реализованы СКЗИ и среда функционирования;

е) возможность располагать аппаратными компонентами СКЗИ и среды функционирования, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

ж) с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и среду функционирования, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО;

з) проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

и) в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и среды функционирования, в том числе с использованием исходных текстов входящего в среду функционирования прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ;

к) создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО;

л) возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты среды функционирования;

м) возможность располагать всеми аппаратными компонентами СКЗИ и среды функционирования;

6. Для обеспечения 4 уровня защищенности персональных данных (при использовании СКЗИ) необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

д) назначении должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе

7. В настоящее время в области обеспечения безопасности персональных данных с использованием средств криптозащиты информации действуют следующие нормативно-методические документы ФСБ России:

а) Приказ ФСБ от 10 июля 2014 года N 378 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности";

б) Приказ ФСБ России от 9 февраля 2005 года N 66 "Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)";

в) "Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну", утвержденная приказом ФАПСИ от 13 июня 2001 года N 152;

г) "Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности", утвержденные руководством 8 Центра ФСБ России (N 149/7/2/6-432 от 31.03.2015);

д) все вышеперечисленные;

8. Чем удостоверяется соответствие средств криптозащиты информации, требованиям по защите информации?

а) аттестатом соответствия;

б) лицензией;

в) сертификатом соответствия;

г) аттестатом аккредитации;

9. Сколько классов средств криптографической защиты информации может применяться для нейтрализации атак, организуемых с целью нарушения безопасности защищаемых персональных данных?

а) два класса;

в) три класса;

г) четыре класса;

д) пять классов;

Задания открытого типа

1. Сколько установлено классов для средств криптозащиты информации?
2. В каких случаях допускается хранение съемных машинных носителей информации персональных данных вне сейфов (металлических шкафов)?
3. В каких информационных системах в целях защиты информации предусмотрено обязательное применение квалифицированной электронной подписи?
4. В информационной системе персональных данных угрозы 1-го типа актуальны, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в
5. В информационной системе персональных данных угрозы 2-го типа актуальны, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в

Задания с развёрнутым ответом

1. Какие основные мероприятия проводятся в государственной информационной системе для формирования требований по защите информации.

Критерии оценивания	Шкала оценок
Обучающийся приводит основные мероприятия защиты информации в государственных информационных системах. Подробно описан каждый из этапов.	Отлично (90-100 баллов)
Обучающийся приводит основные мероприятия защиты информации в государственных информационных системах. Подробно описан каждый из этапов. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Обучающийся допускает ошибку в последовательности основных мероприятий защиты информации в государственных информационных системах. Частично описан каждый из этапов. Ответ не содержит грубых ошибок.	Удовлетворительно (50-70 баллов)
Не представлены этапы формирования требований защиты информации в государственных информационных системах. Присутствуют грубые ошибки или неточности.	Неудовлетворительно

Компетенция ПК-3

Задания закрытого типа

1. Формирование требований к защите информации, содержащейся в государственной информационной системе, предполагает следующие этапы:

а) принятие решения о необходимости защиты информации; классификацию информационной системы по требованиям защиты информации; определение угроз безопасности информации; определение требований к системе защиты информации;

б) анализ рисков нарушения информационной безопасности; разработку модели угроз безопасности информации; определение требований к системе защиты информации;

в) анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система; определение угроз безопасности информации; определение требований к системе защиты информации;

г) определение информации, подлежащей защите в информационной системе и ее значимости; классификации информационной системы по требованиям защиты информации; определение угроз безопасности информации; определение требований к системе защиты информации;

2. Модель угроз безопасности информации и (или) техническое задание на создание государственной информационной системы должны быть согласованы (в пределах их полномочий в части, касающейся выполнения установленных требований о защите информации)

а) ФСТЭК России; ФСБ России; Минцифры России; Роскомнадзор;

б) ФСТЭК России; Роскомнадзор; Минцифры России;

в) ФСТЭК России; ФСБ России; Роскомнадзор;

г) ФСТЭК России; ФСБ России;

д) ФСТЭК России; Минцифры России;

3. Требования к системе защиты информации государственной информационной системы определяются в зависимости от:

а) банка данных угроз безопасности информации (bdu.fstec.ru), а также результатов анализа уязвимостей информационной системы;

б) модели угроз безопасности информации, а также результатов анализа уязвимостей информационной системы;

в) класса защищенности информационной системы и угроз безопасности информации, включенных в модель угроз безопасности информации;

г) от значимости обрабатываемой в ней информации и масштаба информационной системы;

4. В каких информационных системах в целях защиты информации предусмотрено обязательное применение средств криптографической защиты информации?

а) в государственных информационных системах;

б) в информационных системах персональных данных;

в) в информационных системах общего пользования;

г) в информационных системах персональных данных, если персональные данные подлежат криптографической защите в соответствии с законодательством Российской Федерации и осуществляется передача таких персональных данных по не защищенным каналам связи и/или осуществляется хранение персональных данных на носителях информации, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов;

5. В каких информационных системах в целях защиты информации предусмотрено обязательное применение квалифицированной электронной подписи?

а) в государственных информационных системах;

б) в информационных системах персональных данных;

в) в информационных системах общего пользования;

г) во всех перечисленных выше информационных системах;

6. Разработка системы защиты информации информационной системы осуществляется в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным техническим заданием) на создание системы защиты информации информационной системы и включает следующие стадии:

а) классификацию информационной системы по требованиям защиты информации; определение угроз безопасности информации; определение требований к системе защиты информации;

б) разработку модели угроз; определение требований к системе защиты информации; определение видов и типов средств защиты информации, обеспечивающих реализацию технических мер защиты информации; разработку эксплуатационной документации;

в) разработку модели угроз; определение требований к системе защиты информации; определение необходимых средств защиты информации; разработку организационно-распорядительной и эксплуатационной документации;

г) проектирование системы защиты информации; разработку эксплуатационной документации; макетирование и тестирование системы защиты информации (при необходимости);

7. Эксплуатационная документация на систему защиты информации информационной системы разрабатывается с учетом ГОСТ 34.601, ГОСТ 34.201 и ГОСТ Р 51624 и должна в том числе содержать:

- а) руководство пользователя; руководство оператора; руководство администратора; описание правил эксплуатации системы защиты информации информационной системы;
- б) описание структуры системы защиты информации информационной системы; описание состава, мест установки, параметров и порядка настройки средств защиты информации, программного обеспечения и технических средств; описание правил эксплуатации системы защиты;
- в) руководство администратора информационной системы; описание правил развертывания и эксплуатации системы защиты информации информационной системы;
- г) порядок развертывания и настройки средств защиты информации; описание правил эксплуатации системы защиты; правила и требования по реализации установленных мер защиты информации;

8. Внедрение системы защиты информации информационной системы осуществляется в соответствии с проектной и эксплуатационной документацией на систему защиты информации информационной системы и в том числе включает:

- а) настройку средств защиты; предварительные испытания системы защиты информации; опытную эксплуатацию системы защиты информации; приемочные испытания; аттестацию информационной системы;
- б) развертывание средств защиты; разработку организационных мер защиты информации; предварительные испытания системы защиты информации; опытную эксплуатацию системы защиты информации; анализ уязвимостей и принятие мер защиты информации по их устранению; приемочные испытания;
- в) установку и настройку средств защиты; разработку организационно-распорядительных документов по защите информации; внедрение организационных мер защиты информации; предварительные испытания системы защиты информации; опытную эксплуатацию системы защиты информации; анализ уязвимостей и принятие мер защиты информации по их устранению; приемочные испытания;
- г) установку и настройку средств защиты; разработку организационно-распорядительных документов по защите информации; внедрение организационных мер защиты информации; обучение пользователей; предварительные испытания системы защиты информации; опытную эксплуатацию системы защиты информации; приемочные испытания;

9. Разрабатываемые организационно-распорядительные документы по защите информации должны определять правила и процедуры:

- а) управления (администрирования) системой защиты информации; выявления инцидентов безопасности информации и реагирования на них; управления конфигурацией информационной системы и системы защиты информации; контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе; защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации;
- б) управления (администрирования) системой защиты информации; управления конфигурацией информационной системы и системы защиты информации; контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе; защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации;
- в) управления (администрирования) системой защиты информации; управления конфигурацией информационной системы и системы защиты информации; контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;
- г) выявления инцидентов безопасности информации и реагирования на них; управления конфигурацией информационной системы и системы защиты информации; контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;

10. При внедрении организационных мер защиты информации осуществляются:

- а) реализация правил разграничения доступа, установка и настройка средств защиты; разработка организационно-распорядительных документов по защите информации; обучение пользователей; предварительные испытания системы защиты информации; опытная эксплуатация системы защиты информации;
- б) реализация правил разграничения доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения; проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов; отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации;

в) развертывание средств защиты; разработка организационных мер защиты информации; предварительные испытания системы защиты информации; опытную эксплуатацию системы защиты информации; анализ уязвимостей и принятие мер защиты информации по их устранению; приемочные испытания;

г) обучение пользователей; предварительные испытания системы защиты информации; опытная эксплуатация системы защиты информации; анализ уязвимостей и принятие мер защиты информации по их устранению; реализация правил разграничения доступа, и введение ограничений на действия пользователей; проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов; отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации;

Задания открытого типа

1. В каких информационных системах в целях защиты информации предусмотрено обязательное применение квалифицированной электронной подписи?
2. В информационной системе персональных данных угрозы 1-го типа актуальны, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в
3. В информационной системе персональных данных угрозы 2-го типа актуальны, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в
4. Как часто в информационной системе персональных данных должен проводиться контроль выполнения требований защиты информации?
5. Какие классы средств криптозащиты информации требуют контроля целостности программного обеспечения?

Задания с развёрнутым ответом

1. Как происходит признание квалифицированной электронной подписи действительной?

Критерии оценивания	Шкала оценок
Обучающийся приводит алгоритм и перечень всех условий признания квалифицированной электронной подписи действительной.	Отлично (90-100 баллов)
Обучающийся приводит алгоритм и перечень всех условий признания квалифицированной электронной подписи действительной. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Обучающийся допускает ошибку в алгоритме и/или перечне всех условий признания квалифицированной электронной подписи действительной. Ответ не содержит грубых ошибок.	Удовлетворительно (50-70 баллов)
Обучающийся не знает алгоритм и перечень всех условий признания квалифицированной электронной подписи действительной. Присутствуют грубые ошибки или неточности.	Неудовлетворительно

20.2. Промежуточная аттестация

Промежуточная аттестация может включать в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

При оценивании могут использоваться количественные или качественные шкалы оценок.

Для оценивания результатов обучения при проведении промежуточной аттестации используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1) знание нормативных документов, основных определений, понятий и используемой терминологии;

2) умение проводить обоснование требований нормативных документов и практических мер их реализующих с использованием сертифицированных средств защиты информации;

3) умение связывать требования нормативных документов с практикой, иллюстрировать ответ примерами, в том числе, собственными, умение выявлять и анализировать основные закономерности, полученные, в том числе, в ходе выполнения лабораторно-практических заданий;

4) умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу;

5) владение навыками программирования и администрирования компьютерных систем и средств защиты в рамках выполняемых лабораторных заданий;

6) владение навыками проведения компьютерного эксперимента, тестирования компьютерных моделей алгоритмов обработки информации.

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций) на государственном экзамене:

- высокий (углубленный) уровень сформированности компетенций;
- повышенный (продвинутый) уровень сформированности компетенций;
- пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на государственном экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Для оценивания результатов обучения на зачете используется – зачтено, не зачтено по результатам тестирования.

Соотношение показателей, критериев и шкалы оценивания результатов обучения на государственном экзамене представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок на зачете

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	Неудовлетворительно

20.3. Примерный перечень практических заданий, тем рефератов, тем презентаций, докладов, вопросов к зачету с оценкой

№	Содержание
1	Электронная подпись, назначение и применение, история возникновения, используемые алгоритмы. Сертификат ключа проверки электронной подписи. Хранение закрытого ключа.
2	Основные угрозы криптоатак. Инфраструктура открытых ключей (PKI). Удостоверяющий центр. Возможные архитектуры построения PKI..
3	Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи». Виды электронной подписи.
4	Приказ Минкомсвязи России от 23.11.2011 N 320 "Об аккредитации удостоверяющих центров".
5	Приказ ФСБ от 27 декабря 2011 г. N 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».
6	Приказ ФСБ от 27 декабря 2011 г. N 796 «Об утверждении требований к средствам электронной подписи и требованиям к средствам удостоверяющего центра».
7	Минкомсвязь России 13.04.2012 г. Рекомендации по составу квалифицированного сертификата ключа проверки электронной подписи.
8	Криптопровайдеры. Основные технологии, используемые при развёртывании удостоверяющих центров.
9	Развёртывание удостоверяющего центра КриптоПро УЦ. Основные задачи, выполняемые на удостоверяющем центре.
10	Основные требования по безопасности информации на удостоверяющем центре и типовые средства защиты.
11	Носители информации, используемые для электронной подписи и их особенности.
12	Программные средства, использующие электронную подпись. Типовые решения, реализующие возможность применения электронной подписи.
13	Портал государственных услуг Российской Федерации. Универсальная электронная карта.
14	Основные вопросы лицензирования при развёртывании удостоверяющего центра.
15	Регламент работы удостоверяющего центра, основные положения.
16	Список отозванных сертификатов. Основные алгоритмы формирования и проверки актуальности.
17	Угрозы безопасности информации и основные направления защиты, связанные с использованием электронной подписи.
18	Основные технологии и средства защиты информации, применяемые при развёртывании удостоверяющего центра.
19	Проблемные вопросы безопасности информации при использовании квалифицированной электронной подписи.
20	Архитектура программного обеспечения и ее связь с технологией блокчейна. Преимущества и недостатки распределенных систем. Реализация и поддержка целостности в распределенных системах.
21	Обеспечение доверительности и целостности в распределенных системах. Право владения и блокчейн. Проблема двойного расходования.
22	Примеры структур данных и алгоритмов, применяемых для реализации блокчейн технологий.
23	Перспективы и практическое использование блокчейн технологий

20.4. Пример задания для выполнения лабораторной работы

Лабораторная работа №4

Развертывание удостоверяющего центра Крипто-Про УЦ.

Цель работы: практическое изучение особенностей использования программного обеспечения Крипто-Про для реализации методов защиты информации с использованием электронной подписи.

20.5. Пример контрольно-измерительного материала

УТВЕРЖДАЮ

Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота
 __.__.2027

Направление подготовки / специальность 10.05.01 Компьютерная безопасность

Дисциплина Б1.В.03 Технологии защищенного документооборота и блокчейн

Форма обучения Очное

Вид контроля Зачет

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Электронная подпись, назначение и применение, история возникновения, используемые алгоритмы. Сертификат ключа проверки электронной подписи. Хранение закрытого ключа.
2. Проблемные вопросы безопасности информации при использовании квалифицированной электронной подписи.

Преподаватель _____ С.А. Вялых