Минобрнауки России
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00A29CA99D98126F4EB57F6F989D713C88
Владелец: Василенко Виталий Николаевич
Действителен: с 07.07.2022 до 30.09.2023

УТВЕРЖДАЮ
Проректор по учебной работе

_____ Василенко В.Н.
(подпись) (Ф.И.О.)

«25» мая 2023

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Технологии разработки защищенного документооборота

Специальность

10.05.03 Информационная безопасность автоматизированных систем

Специализация

Безопасность открытых информационных систем

Квалификация выпускника

специалист по защите информации

1. Цели и задачи дисциплины

Целями освоения дисциплины «Технология разработки защищенного документооборота» являются теоретическая и практическая подготовка специалистов к деятельности, связанной с комплексным анализом возможных угроз и созданием адекватной модели нарушителя, постановкой конкретных задач заданной степени сложности в рамках модели для обеспечения информационной безопасности автоматизированных систем, а также содействие фундаментализации образования и развитию системного мышления.

Задачи дисциплины «Технологии разработки защищенного документооборота» в научно-исследовательской деятельности:

- сбор, обработка, анализ и систематизация научно-технической информации по проблематике информационной безопасности автоматизированных систем;
- подготовка научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований;
- разработка эффективных решений по обеспечению информационной безопасности автоматизированных систем.

Объектами профессиональной деятельности являются:

– автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите;

– информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите;

– технологии обеспечения информационной безопасности автоматизированных систем;

– системы управления информационной безопасностью автоматизированных систем.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины в соответствии с предусмотренными компетенциями обучающийся должен:

№ п/ п	Код компетенции	Содержание компетенции (результат освоения)	В результате изучения учебной дисциплины обучающийся должен:		
			знать	уметь	владеть
1	ОК-2	способностью использовать основы экономических знаний в различных сферах деятельности	о современных направлениях развития и совершенствования процессов управления экономическими, социальными и производственными процессами в организационных структурах различных типов и форм собственности;	организовывать работу руководителей, специалистов и технического персонала с документами в системах электронного документооборота	владеть современными технологиями управления персоналом
2	ОК-4	способностью использовать основы правовых	правовые основы защиты конфиденциальной	использовать в профессиональной деятельности	Методиками модернизации, унификации

		знаний в различных сферах деятельности	информации по видам тайны; правовые основы деятельности подразделений защиты информации; порядок лицензирования деятельности по технической защите конфиденциальной информации;	нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;	систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России. ФСТЭК России
3	ОК-5	способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	порядок отнесения информации к разряду конфиденциальной информации; порядок разработки, учета, хранения, размножения и уничтожения конфиденциальных документов; порядок допуска и доступа персонала к защищаемым сведениям; правовое регулирование взаимоотношений администрации и персонала в области защиты информации;	применять полученные знания и навыки в своей дальнейшей профессиональной деятельности	навыками создания и использования систем электронного документооборота и организации их защиты
4	ОПК-4	способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах	тенденции развития информационных технологий, необходимых для поиска информации в компьютерных системах, сетях, библиотечных фондах	использовать современные защищенные информационные технологии. для поиска информации в компьютерных системах, сетях, библиотечных фондах	навыками использования новейших информационных технологий; передового отечественного и зарубежного опыта по разработке автоматизированных систем управления технологическими процессами, фограммными средствами визуального представления

5	ОПК-5	способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	правовые нормы в области защиты интеллектуальной собственности;	разрабатывать эффективные технологические схемы рационального документооборота с использованием современных систем и способов обработки и хранения конфиденциальных документов;	обработкой и сравнительным анализом справочной и реферативной информации,
6	ОПК-6	способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	организацию работы руководителей, специалистов и технического персонала с конфиденциальными документами на любом носителе информации	руководить службой конфиденциальной документации	Навыками организации работы малых коллективов исполнителей по защите электронной документации
7	ПК-2	Способностью создавать и исследовать модели автоматизированных систем	современные системы электронного документооборота, основные тенденции развития автоматизированных систем и способов обработки и хранения конфиденциальных документов, а также совершенствования носителей документной информации.	практически выполнять технологические операции по защите и обработке документов в системах электронного документооборота	методами управления электронного документооборота
8	ПК-7	способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области	разрабатывать и оформлять нормативно-методические материалы по регламентации процессов обработки, храпения и защиты конфиденциальных документов	способностью к контролю соответствия разрабатываемых проектов и технической документации стандартам, техническим условиям и другим нормативным документам

9	ПК-8	способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	организацию конфиденциального документооборота; технологию работы с конфиденциальными документами; организацию электронного документооборота	определять состав документированной конфиденциальной информации; подготавливать, издавать и учитывать конфиденциальные документы;	способностью к разработке проектной и рабочей технической документации, оформлению законченных проектных работ в соответствии с нормами и стандартами;
10	ПК-9	способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	существующие типы автоматизированных систем и способы обработки и хранения конфиденциальных документов, функциональных возможности этих систем, номенклатуре вычислительной и организационной техники	формулировать задачи по разработке потребительских требований к автоматизированны м системам обработки и хранения электронных документов;	навыками работы с информационн ыми системами электронного документообор ота
11	ПК-21	способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	основы разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации	способностью к разработке программ и методик испытаний средств и систем обеспечения информационн ой безопасности.

3. Место дисциплины в структуре ОП ВО

Дисциплина «Технология разработки защищенного документооборота» относится к блоку 1 ОП ВО и ее вариативной части.

Изучение дисциплины основано на знаниях, умениях и навыках, полученных при изучении обучающимися дисциплин и прохождении практик:

– Технологии и методы программирования;

– Учебная практика, практика по получению первичных профессиональных умений.

Дисциплина является предшествующей для изучения дисциплин, прохождения практик:

– Мультимедиатехнологии;

– Учебная практика, практика по получению первичных умений и навыков научно-исследовательской деятельности;

– Производственная практика, практика по получению профессиональных умений и опыта профессиональной деятельности;

– Производственная практика, преддипломная практика;

защиты выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

4. Объем дисциплины и виды учебных занятий

Общая трудоемкость дисциплины составляет 7 зачетных единиц.

Виды учебной работы	Всего часов	Семестр	
		4	5
	акад. ч	акад. ч	акад. ч
Общая трудоемкость дисциплины	**252**	**108**	**144**
Контактная работа, в т.ч. аудиторная работа	**134,45**	**55**	**79,45**
Лекции	33	18	15
в том числе в форме практической подготовки	–	–	–
Лабораторные работы (ЛР)	30	–	30
в том числе в форме практической подготовки	30	–	30
Практические занятия (ПЗ)	66	36	30
в том числе в форме практической подготовки	66	36	30
Консультации текущие	1,65	0,9	0,75
Консультации по контрольной работе	1,5	–	1,5
Проведение консультаций перед экзаменом	2	–	2
Вид контроля – зачет, экзамен	0,3	0,1	0,2
Самостоятельная работа (СР)	**83,75**	**53**	**30,75**
Подготовка доклада с презентацией	20	20	–
Домашнее задание	33	33	–
Курсовая работа	30,75	–	30,75
Подготовка к экзамену (контроль)	**33,8**	**–**	**33,8**

5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1 Содержание разделов дисциплины

№ п/п	Наименование разделов дисциплины	Содержание раздела	Трудоемкость раздела, час
1	Основные понятия и определения электронного документооборота. Федеральный закон об электронной подписи	Основные понятия и определения электронного документооборота. Федеральный закон об электронной подписи	18
2	Организационно-технические и правовые основы использования электронного документооборота и ЭП в информационных системах	Работа с документами в организации. “Электронная революция” в работе с документами. Особенности рынка систем управления деловыми процессами. Составляющие экономического эффекта	20
3	Международные стандарты делопроизводства и документооборота	Стандарты ISO серии 9000. Стандарт ISO15489. DoD 5015.2.	23
4	Традиционные бумажные и электронные документы	Документ на бумажном носителе и рукописная подпись. Электронные документы. Важнейшие реквизиты электронного документооборота. Угрозы безопасности субъектам электронного документооборота.	23
5	Электронная цифровая подпись	Определение и функции электронной цифровой подписи	23
6	Криптографические методы защиты информации	Задачи решаемые криптографическими технологиями защиты информации. Криптография с симметричными ключами. Криптография с открытыми ключами. Криптография с открытым ключом и Хэш-функция в схеме электронной цифровой подписи	14

7	Электронные сертификаты	Определение электронных сертификатов Сертификаты X.509. Классы сертификатов. Хранилища сертификатов. Импорт и экспорт сертификатов	16
8	CryptoAPI и криптопровайдеры	Архитектура CryptoAPI. Определение и функции криптопровайдера	18
9	КриптоПро CSP и TLS	Назначение СКЗИ КриптоПРО CSP. Типы ключевых носителей. Основные функции реализуемые КриптоПро CSP. КриптоПро TLS. ETOKEN. Жизненный цикл eToken PRO. Cryptography Next Generation API (CNG). Архитектура CNG API	20
10	Public Key Infrastructure (PKI)	Определение и цели применения PKI. Компоненты PKI. Принципы доверия PKI	12
11	КриптоПро OCSP Server и КриптоПро TSP Server. Усовершенствованная подпись КриптоПро	Назначение и характеристики КриптоПро OCSP Server. КриптоПро Revocation Provider. Назначение КриптоПро TSP Server. Схема усовершенствованной подписи КриптоПро. Технологические процедуры. Создание усовершенствованной электронной цифровой подписи	12
12	ЭЦП в PKI на основе Удостоверяющего центра КриптоПро	Основные возможности, назначение и применение «Удостоверяющего Центра КриптоПро УЦ». Формат и состав сертификатов, поддерживаемых «КриптоПро УЦ». Основные расширения CLR	13,75

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, час	ЛР, час	ПЗ, час	СР, час
1	Основные понятия и определения электронного документооборота. Федеральный закон об электронной подписи	2	–	6	10
2	Организационно-технические и правовые основы использования электронного документооборота и ЭП в информационных системах	4	–	6	10
3	Международные стандарты делопроизводства и документооборота	4	–	8	11
4	Традиционные бумажные и электронные документы	4	–	8	11
5	Электронная цифровая подпись	4	–	8	11
6	Криптографические методы защиты информации	2	4	6	2
7	Электронные сертификаты	2	4	4	6
8	CryptoAPI и криптопровайдеры	2	6	4	6
9	КриптоПро CSP и TLS	2	4	4	10
10	Public Key Infrastructure (PKI)	2	4	4	2
11	КриптоПро OCSP Server и КриптоПро TSP Server. Усовершенствованная подпись КриптоПро	2	4	4	2
12	ЭЦП в PKI на основе Удостоверяющего центра КриптоПро	3	4	4	2,75

5.2.1Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, Час
1	Основные понятия и определения электронного документооборота. Федеральный закон об электронной подписи	Основные понятия и определения электронного документооборота. Федеральный закон об электронной подписи	2

2	Организационно-технические и правовые основы использования электронного документооборота и ЭП в информационных системах	Работа с документами в организации. “Электронная революция” в работе с документами. Особенности рынка систем управления деловыми процессами. Составляющие экономического эффекта	4
3	Международные стандарты делопроизводства и документооборота	Стандарты ISO серии 9000. Стандарт ISO15489. DoD 5015.2.	4
4	Традиционные бумажные и электронные документы	Документ на бумажном носителе и рукописная подпись. Электронные документы. Важнейшие реквизиты электронного документооборота. Угрозы безопасности субъектам электронного документооборота.	4
5	Электронная цифровая подпись	Определение и функции электронно-цифровой подписи	4
6	Криптографические методы защиты информации	Задачи решаемые криптографическими технологиями защиты информации. Криптография с симметричными ключами. Криптография с открытыми ключами. Криптография с открытым ключом и Хэш-функция в схеме электронной цифровой подписи	2
7	Электронные сертификаты	Определение электронных сертификатов. Сертификаты X.509. Классы сертификатов. Хранилища сертификатов. Импорт и экспорт сертификатов	2
8	CryptoAPI и криптопровайдеры	Архитектура CryptoAPI. Определение и функции криптопровайдера	2
9	КриптоПро CSP и TLS	Назначение СКЗИ КриптоПРО CSP. Типы ключевых носителей. Основные функции реализуемые КриптоПро CSP. КриптоПро TLS. ETOKEN. Жизненный цикл eToken PRO. Cryptography Next Generation API (CNG). Архитектура CNG API	2
10	Public Key Infrastructure (PKI)	Определение и цели применения PKI. Компоненты PKI. Принципы доверия PKI	2
11	КриптоПро OCSP Server и КриптоПро TSP Server. Усовершенствованная подпись КриптоПро	Назначение и характеристики КриптоПро OCSP Server. КриптоПро Revocation Provider. Назначение КриптоПро TSP Server. Схема усовершенствованной подписи КриптоПро. Технологические процедуры. Создание усовершенствованной электронной цифровой подписи	2
12	ЭЦП в PKI на основе Удостоверяющего центра КриптоПро	Основные возможности, назначение и применение «Удостоверяющего Центра КриптоПро УЦ». Формат и состав сертификатов, поддерживаемых «КриптоПро УЦ». Основные расширения CLR	3

5.2.2 Практические занятия

№ п/п	Наименование раздела дисциплины	Тематика практических занятий	Трудоемкость, час
1	Основные понятия и определения электронного документооборота. Федеральный закон об электронной подписи	Создание самоподписанного сертификата. Получение сертификата с помощью утилиты МакеCert Изучение структуры полученного сертификата с помощью оснастки MMC.	6
2	Организационно-технические и правовые основы использования электронного документооборота и ЭП в	Настройка WEBинтерфейса. Создание ресурса Public и настройка интерфейса Web Enrollment Support	6

	информационных системах		
3	Международные стандарты делопроизводства и документооборота	КриптоАРМ. Изучение процедуры установки КриптоАРМ	8
4	Традиционные бумажные и электронные документы	Создание самоподписанного сертификата с помощью КриптоАРМ. Изучение процесса создания самоподписанного сертификатат с использованием прикладного ПО с графическим интерфейсом	8
5	Электронная цифровая подпись	Настройка подчиненного СА. Изучение процедуры запуска и настройки подчиненного СА	8
6	Криптографические методы защиты информации	Защитить сайт на IIS с помощью ssl туннеля. Настроить аутентификацию пользователей по сертификату на этом сайте, используя сервера. Выдать пользователю сертификат, проверить, что пользователь с этим сертификатом заходит, а если у пользователя сертификата нет то он не зайдёт. Сертификаты раздаются при помощи УЦ, настроенного в лабораторной работе №2. Отозвать сертификат в удостоверяющем центре и проверить, что пользователь не может зайти на сайт.	6
7	Электронные сертификаты	Импорт и экспорт сертификатов. Изучение режима генерации и хранения ключей на компьютере. Изучение процедур экспорта и импорта сертификатов, как меры повышения безопасности использования секретных ключей. Изучение возможности привязки секретных ключей к ключевому носителю	4
8	CryptoAPI и криптопровайдеры	Получение сертификатов с использованием СКЗИ КриптоПро. Изучение процедуры получения сертификатов с использованием СКЗИ КриптоПро	4
9	КриптоПро CSP и TLS	СКЗИ КриптоПро. Изучение процедуры установки и настройки криптопровайдера СКЗИ КриптоПро	4
10	Public Key Infrastructure (PKI)	Построение PKI. Изучение процедуры построения иерархической PKI	4
11	КриптоПро OCSP Server и КриптоПро TSP Server. Усовершенствованная подпись КриптоПро	Управление доверием на стороне пользователя. Изучение процедуры установления доверия в иерархии PKI.	4
12	ЭЦП в PKI на основе Удостоверяющего центра КриптоПро	TSP сервер и OCSP сервер. TSP сервер (cryptopro tsp server, либо служба меток времени в 2008 сервере). Отправляем файл на сервер, который ставит метку времени на файл, после чего пользователь ставит на этот файл свою подпись. OCSP сервер. (online sertificate status protocol)На отдельном сервере CSP сервер, на клиенте relocation provider. Выдать сертификат, отозвать его и проверить, что не работает.	4

5.2.3 Лабораторный практикум

№ п/п	Наименование раздела дисциплины	Тематика лабораторных работ	Трудоемкость, час
1	Основные понятия и определения электронного документооборота. Федеральный закон об электронной подписи	–	–
2	Организационно-технические и правовые основы использования электронного документооборота и ЭП в информационных системах	–	–

3	Международные стандарты делопроизводства и документооборота	–	–
4	Традиционные бумажные и электронные документы	–	–
5	Электронная цифровая подпись	–	–
6	Криптографические методы защиты информации	Построение системы электронного документооборота: определение связей, детализация моделей.	4
7	Электронные сертификаты	Построение системы электронного документооборота: построение структуры, определение методов	4
8	CryptoAPI и криптопровайдеры	Построение системы электронного документооборота: построение математической модели обеспечения безопасности рабочего потока	6
9	КриптоПро CSP и TLS	Построение системы электронного документооборота: организация поддержки обращений пользователей с учетом особенностей электронного представления документа	4
10	Public Key Infrastructure (PKI)	Построение системы электронного документооборота: управление данными, многоуровневая структура	4
11	КриптоПро OCSP Server и КриптоПро TSP Server. Усовершенствованная подпись КриптоПро	Построение системы электронного документооборота: организация рабочих потоков в сети	4
12	ЭЦП в PKI на основе Удостоверяющего центра КриптоПро	Построение системы электронного документооборота: организация защиты потока данных от внешних воздействий	4

5.2.4Самостоятельная работа обучающихся (СРО)

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, час
1	Основные понятия и определения электронного документооборота. Федеральный закон об электронной подписи	Подготовка доклада с визуальным представлением	10
2	Организационно-технические и правовые основы использования электронного документооборота и ЭП в информационных системах		10
3	Международные стандарты делопроизводства и документооборота	Домашнее задание	11
4	Традиционные бумажные и электронные документы		11
5	Электронная цифровая подпись		11
6	Криптографические методы защиты информации	Курсовая работа	2
7	Электронные сертификаты		6
8	CryptoAPI и криптопровайдеры		6
9	КриптоПро CSP и TLS		10
10	Public Key Infrastructure (PKI)		2
11	КриптоПро OCSP Server и КриптоПро TSP Server. Усовершенствованная подпись КриптоПро		2
12	ЭЦП в PKI на основе Удостоверяющего центра КриптоПро		2,75

6 Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература

1. Куняев, Н. Н. Конфиденциальное делопроизводство и защищенный электронный документооборот : учебник / Н. Н. Куняев ; под редакцией Н. Н. Куняева. – 2-е изд., перераб. и доп. – Москва : Логос, 2020. – 500 с. – ISBN 978-5-

98704-711-8. – Текст : электронный // Лань : электронно-библиотечная система. – Режим доступа: https://e.lanbook.com/book/163041.

2. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений : учебное пособие для вузов / С. Н. Никифоров. – 4-е изд., стер. – Санкт-Петербург : Лань, 2022. – 96 с. – ISBN 978-5-8114-9562-7. – Текст : электронный // Лань : электронно-библиотечная система. – Режим доступа: https://e.lanbook.com/book/200480.

3. Методы и средства комплексной защиты информации в технических системах : учебное пособие / Э. В. Запонов, А. П. Мартынов, И. Г. Машин [и др.]. – Саров : РФЯЦ- ВНИИЭФ, 2019. – 224 с. – ISBN 978-5-9515-0429-6. – Текст : электронный // Лань : электронно-библиотечная система. – Режим доступа: https://e.lanbook.com/book/243467.

4. Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. – Ростов-на-Дону : Донской ГТУ, 2021. – 228 с. – ISBN 978-5-7890-1878-1. – Текст : электронный // Лань : электронно-библиотечная система. – Режим доступа: https://e.lanbook.com/book/237770.

6.2 Дополнительная литература

1. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. – 3-е изд., перераб. – Санкт-Петербург : Лань, 2021. – 236 с. – ISBN 978-5-8114-5632-1. – Текст : электронный // Лань : электронно-библиотечная система. – Режим доступа: https://e.lanbook.com/book/156401.

2. Гусарова, М. Н. Электронные офисные системы : учебно-методическое пособие / М. Н. Гусарова, О. Г. Савка, Л. И. Горелова. – Москва : РТУ МИРЭА, 2021. – 88 с. – Текст : электронный // Лань : электронно-библиотечная система. – Режим доступа: https://e.lanbook.com/book/176561.

3. Автоматизация документооборота : учебное пособие / А. А. Тищенко, Ю. М. Казаков, М. В. Терехов [и др.]. – Москва : ФЛИНТА, 2018. – 108 с. – ISBN 978-5-9765-4024-8. – Текст : электронный // Лань : электронно-библиотечная система. – Режим доступа: https://e.lanbook.com/book/113481.

4. Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А. М. Голиков. – Москва : ТУСУР, 2015. – 284 с. – Текст : электронный // Лань : электронно-библиотечная система. – Режим доступа: https://e.lanbook.com/book/110336.

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

Технология разработки защищенного документооборота [Электронный ресурс] : методические указания для самостоятельной работы для студентов, обучающихся по направлению 10.05.03 – «Информационная безопасность автоматизированных систем», очной формы обучения / А. В. Скрыпников, Е. В. Чернышова ; ВГУИТ, Кафедра информационной безопасности. - Воронеж : ВГУИТ, 2016. - 16 с. - Электрон. ресурс. http://biblos.vsuet.ru/ProtectedView/Book/ViewBook.

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

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
«Российское образование» - федеральный портал	*https://www.edu.ru/*
Научная электронная библиотека	*https://elibrary.ru/defaultx.asp*
Национальная исследовательская компьютерная сеть России	*https://niks.su/*

Информационная система «Единое окно доступа к образовательным ресурсам»	*http://window.edu.ru/*
Электронная библиотека ВГУИТ	*http://biblos.vsuet.ru/megapro/web*
Сайт Министерства науки и высшего образования РФ	*https://minobrnauki.gov.ru/*
Портал открытого on-line образования	*https://npoed.ru/*
Электронная информационно-образовательная среда ФГБОУ ВО «ВГУИТ»	*https://education.vsuet.ru/*

6.5 Методические указания для обучающихся по освоению дисциплины

Методические указания для обучающихся по освоению дисциплин (модулей) в ФГБОУ ВО ВГУИТ [Электронный ресурс] : методические указания для обучающихся на всех уровнях высшего образования / М. М. Данылив, Р. Н. Плотникова; ВГУИТ, Учебнометодическое управление. Воронеж : ВГУИТ, 2016. – Режим доступа : http://biblos.vsuet.ru/MegaPro/Web/SearchResult/MarcFormat/100813. Загл. с экрана

6.6 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Microsoft Office Professional Plus 2010. Блок управления комплекса радиоконтроля и поиска радиопередающих устройств «ОМЕГА» (переносной), МУ защиты ресурсов сети от внутренних и внешних атак CISCO ASA5505-KB, переносной комплекс для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ

«НАВИГАТОР-ПЗГ»; средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «СОНАТА-РЗ.1»; система защиты речевой информации «Соната-АВ-4Б» (Центральный блок питания и управления + Размыкатели в составе СВАЗ Соната АВ); профессиональный обнаружитель скрытых видеокамер СОКОЛ-М (переносной); портативный обнаружитель закладок Protect1203 (переносной); устройство активной защиты информации «ВЕТО-М»; электронный замок Samsung SHS2920. Страж NT вер.3.0 Сертификат ФСТЭК № 2145 30.07.2013 г.; Ревизор 1XP Сертификат ФСТЭК № 989 08.02.2015 г.; Ревизор 2XP Сертификат ФСТЭК № 990 08.02.2015 г.; Фикс 2.0.2 Сертификат ФСТЭК №1548 15.01.2015 г.; Ревизор сети вер.3.0 Сертификат ФСТЭК №3413 02.06.2015 г.; СЗИ Панцирь К Сертификат ФСТЭК №1973 09.12.2015 г.;

СЗИ Dallas Lock 8.0 К Сертификат ФСТЭК №2720 25.09.2015; СЗИ Dallas Lock 8.0 С Сертификат ФСТЭК №2945 16.08.2013.

7. Материально-техническое обеспечение дисциплины

Аудитории для проведения занятий **лекционного** типа, лабораторных и практических занятий	Ауд. 420: Комплекты мебели для учебного процесса. ПЭВМ – 11 (компьютер Core i5-4460 – 10, Core i5-4570 – 1), рабочая станция РЕГАРД РДЦБ Core i5-8400 – 1 шт., проектор Acer projector X1383WH, экран, стенды – 5 шт., блок управления комплекса радиоконтроля и поиска радиопередающих устройств «ОМЕГА» (переносной), МУ защиты ресурсов сети	Microsoft Windows 7 (академическая лицензия); Microsoft Office (standart) 2007; Microsoft Access 2007; Microsoft Project 2007; Microsoft Share Point 2007; Microsoft Visio 2007; Microsoft SQL server 2008; 7-Zip File Manager (архиватор); Adobe Acrobat Reader; Adobe Flash Player; FAR file manager; Google Chrome; Java TM 7 (64-bit); K-Lite Codec Pack; Mozilla Firefox; Oracle VM VirtualBox;

	от внутренних и внешних атак CISCO ASA5505-KB, переносной комплекс для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ «НАВИГАТОР-ПЗГ»; средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «СОНАТА-Р3.1»; система защиты речевой информации «Соната-АВ-4Б» (Центральный блок питания и управления + Размыкатели в составе СВАЗ Соната АВ); профессиональный обнаружитель скрытых видеокамер СОКОЛ-М (переносной); портативный обнаружитель закладок Protect1203 (переносной); устройство активной защиты информации «ВЕТО-М»; электронный замок Samsung SHS-2920; средство активной защиты информации изделие «Салют 2000С» с регулятором выходного уровня шума	Sublime Text; Symantec Endpoint Protection 12 (Заменен на AVP Kaspersky); VMWare Player; Антивирус “Зоркий глаз”; Lazarus; SmathStudio; NanoCAD; Gimp (графический редактор, аналог Photoshop); Avidemax (видео редактор); Virtual Dub (видео редактор); Free Pascal; Страж NT вер.4.0 Сертификат ФСТЭК № 2145 30.07.2013 г.; Ревизор 1XP Сертификат ФСТЭК № 989 08.02.2015 г.; Ревизор 2XP Сертификат ФСТЭК № 990 08.02.2015 г.; Фикс 2.0.2 Сертификат ФСТЭК №1548 15.01.2015 г.; Ревизор сети вер.3.0 Сертификат ФСТЭК №3413 02.06.2015 г.; СЗИ Панцирь К Сертификат ФСТЭК №1973 09.12.2015 г.; СЗИ Dallas Lock 8.0 К Сертификат ФСТЭК №2720 25.09.2015; СЗИ Dallas Lock 8.0 С Сертификат ФСТЭК №2945 16.08.2013
Аудитории для проведения занятий лекционного типа, **лабораторных и практических** занятий	Ауд. 332а: Комплекты мебели для учебного процесса. ПЭВМ – 12 (компьютер Core i5-4570), стенды – 5 шт. Ауд. 424: Комплекты мебели для учебного процесса. ПЭВМ – 12: Моноблоки ГРАВИТОН М 40И Intel Pentium ® Gold G5420 CPU – 12 шт..; стенды – 3 Ауд. 420: Комплекты мебели для учебного процесса. ПЭВМ – 11 (компьютер Core i5-4460 – 10, Core i5-4570 – 1), рабочая станция РЕГАРД РДЦБ Core i5-8400 – 1 шт проектор Acer projector X1383WH, экран, стенды – 5 шт., блок управления комплекса радиоконтроля и поиска радиопередающих устройств «ОМЕГА» (переносной), МУ защиты ресурсов сети от внутренних и внешних атак CISCO ASA5505-KB, переносной комплекс для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ «НАВИГАТОР-ПЗГ»; средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «СОНАТА-Р3.1»; система защиты речевой информации «Соната-АВ-4Б» (Центральный блок питания и управления + Размыкатели в составе СВАЗ Соната АВ); профессиональный обнаружитель скрытых видеокамер СОКОЛ-М (переносной); портативный обнаружитель закладок Protect1203 (переносной); устройство активной защиты информации «ВЕТО-М»; электронный замок Samsung SHS-2920	Ауд.332а: ОС Alt Linux (Альт Образование 8.2) Geany. Lazarus. Qt Creator. Quanta Plus. Веб-редактор Bluefish. Среда разработки Code::Blocks. Офисный пакет Libre Office 5.4: Base, Calc, Draw, Impress, Math, Writer. Персональная бухгалтерия HomeBank. Словарь Star Dict. iTest. VM Maxima. Кумир. Avidemux. Audacios. Brasero. Cheese. SMPlayer. Медиаплеер Parole. Редактор тегов Easy TAG. Stath Studio. Pinta. Веб-браузер Mozilla Firefox. Графический редактор. FP – free Pascal. Ауд.424: ОС Alt Linux (Альт Образование 8.2) Geany. Lazarus. Qt Creator. Quanta Plus. Веб-редактор Bluefish. Среда разработки Code::Blocks. Офисный пакет Libre Office 5.4: Base, Calc, Draw, Impress, Math, Writer. Персональная бухгалтерия HomeBank. Словарь Star Dict. iTest. VM Maxima. Кумир. Avidemux. Audacios. Brasero. Cheese. SMPlayer. Медиаплеер Parole. Редактор тегов Easy TAG. Stath Studio. Pinta. Веб-браузер Mozilla Firefox. Графический редактор. FP – free Pascal. Ауд.420: Microsoft Windows 7 (академическая лицензия) Microsoft Office (standart) 2007; Microsoft Access 2007; Microsoft Project 2007; Microsoft Share Point 2007; Microsoft Visio 2007; Microsoft SQL server 2008; 1 С Предприятие Лицензия; 7-Zip File Manager (архиватор); Adobe Acrobat Reader; Adobe Flash Player; FAR file manager; Google Chrome; Java TM 7 (64-bit); K-Lite Codec Pack; Mozilla Firefox;

		Oracle VM VirtualBox; Sublime Text; Symantec Endpoint Protection 12 (Заменен на AVP Kaspersky); VMWare Player; Антивирус “Зоркий глаз”; Lazarus; SmathStudio; NanoCAD; Gimp (графический редактор, аналог Photoshop); Avidemax (видео редактор); Virtual Dub (видео редактор); Free Pascal; Страж NT вер.3.0 Сертификат ФСТЭК № 2145 30.07.2013 г.; Ревизор 1XP Сертификат ФСТЭК № 989 08.02.2015 г.; Ревизор 2XP Сертификат ФСТЭК № 990 08.02.2015 г.; Фикс 2.0.2 Сертификат ФСТЭК №1548 15.01.2015 г.; Ревизор сети вер.3.0 Сертификат ФСТЭК №3413 02.06.2015 г.; СЗИ Панцирь К Сертификат ФСТЭК №1973 09.12.2015 г.; СЗИ Dallas Lock 8.0 К Сертификат ФСТЭК №2720 25.09.2015; СЗИ Dallas Lock 8.0 С Сертификат ФСТЭК №2945 16.08.2013
Аудитории для **самостоятельной** работы, курсового и дипломного проектирования	Читальные залы библиотеки: Компьютеры со свободным доступом в сеть Интернет и Электронными библиотечными и информационно справочными системами; Ауд. 424: Комплекты мебели для учебного процесса. ПЭВМ – 1.; Моноблоки ГРАВИТОН М 40И Intel Prntium ® Gold G5420 CPU – 12 шт..; 3 стенда.	Microsoft Office Professional Plus 2010 Russian Academic OPEN 1 License No Level #61181017 от 20.11.2012 г. http://eopen.microsoft.com. Автоматизированная интегрированная библиотечная система «МегаПро», Номер лицензии: 104-2015, Дата: 28.04.2015. Договор №2140 от 08.04.2015 г. Уровень лицензии «Стандарт» ОС Alt Linux (Альт Образование 8.2) Geany. Lazarus. Qt Creator. Quanta Plus. Веб-редактор Bluefish. Среда разработки Code::Blocks. Офисный пакет Libre Office 5.4: Base, Calc, Draw, Impress, Math, Writer. Персональная бухгалтерия HomeBank. Словарь Star Dict. iTest. VM Maxima. Кумир. Avidemux. Audacios. Brasero. Cheese. SMPlayer. Медиаплеер Parole. Редактор тегов Easy TAG. Stath Studio. Pinta. Веб-браузер Mozilla Firefox. Графический редактор. FP – free Pascal.
Помещения для хранения и проф. обслуживания учебного оборудования	Ауд.423: ПЭВМ-3 (компьютер Core i5-4570 – 1 шт, компьютер Core i5-4460 – 1 шт., рабочая станция РЕГАРД РДЦБ Core i5-8400 – 1 шт , ноутбук 15,6HP, принтер Brother HL-2132, сетевой накопитель Dlink DNS-346	Windows 7 (академическая лицензия) MS Office 2007 (open)

8 Оценочные материалы для промежуточной аттестации обучающихся по дисциплине

8.1 **Оценочные материалы** (ОМ) для дисциплины включают:

- перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;

- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;

- 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;

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

8.2 Для каждого результата обучения по дисциплине определяются показатели и критерии оценивания сформированности компетенций на различных этапах их формирования, шкалы и процедуры оценивания.

ОМ представляются отдельным комплектом и **входят в состав рабочей программы дисциплины**.

Оценочные материалы формируются в соответствии с П ВГУИТ «Положение об оценочных материалах».

Документ составлен в соответствии с требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем и специализации Безопасность открытых информационных систем.

ОЦЕНОЧНЫЕМАТЕРИАЛЫ
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине

Технологии разработки защищенного документооборота

1 Требования к результатам освоения дисциплины

№п/п	Код компетенции	Содержание компетенции (результат освоения)	В результате изучения учебной дисциплины обучающийся должен:		
			знать	уметь	владеть
2	ПК-2	способностью создавать и исследовать модели автоматизированных систем	современные системы электронного документооборота	практически выполнять технологические операции по защите и обработке документов в системах электронного документооборота	методами управления электронного документооборота

2 Паспорт фонда оценочных средств по дисциплине

Контролируемые модули/разделы/темы дисциплины	Индекс контролируемой компетенции (или ее части)	Оценочные средства	Технология оценки (способ контроля)
1. Основные понятия и определения электронного документооборота. Федеральный закон об электронной подписи. 2. Организационно-технические и правовые основы использования электронного документооборота и ЭП в информационных системах 3. Международные стандарты делопроизводства и документооборота. 4. Традиционные бумажные и электронные документы. 5. Электронная цифровая подпись 6. Криптографические методы защиты информации. 7. Электронные сертификаты. 8. CryptoAPI и криптопровайдеры. 9. КриптоПро CSP и TLS. 10. Public Key Infrastructure (PKI). 11. КриптоПро OCSP Server и КриптоПро TSP Server. Усовершенствованная подпись КриптоПро. 12. ЭЦП в PKI на основе Удостоверяющего центра КриптоПро	ПК-3	Зачет	Собеседование
		Контрольные вопросы к текущим опросам на практических работах	Собеседование
		Доклад	Доклад, презентация
		Зачет	Собеседование
		Контрольные вопросы к текущим опросам на практических работах	Собеседование
		ДЗ	Письменная работа
		Экзамен	Собеседование
		Контрольные вопросы к текущим опросам на практических работах	Собеседование
		Вопросы при защите лабораторных работ	Собеседование
		Курсовая работа	Защита курсовой работы

Оценочные средства для промежуточной аттестации

3.1 Вопросы к зачету

ПК-2 - способностью создавать и исследовать модели автоматизированных систем

№ задания	Формулировка вопроса
1.	Федеральный закон об электронной цифровой подписи ФЗ-1.
2.	Система электронного документооборота (определение, назначение, экономический эффект, стандарты ISO серии 9000, ISO 15489, DoD 5015.2, примеры СЭД).
3.	Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной под-

	писи".
4.	Особенности юридического определения ЭЦП в РФ.
5.	Положение о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами.
6.	Положение ПЗК-2005 «о разработке, производстве, реализации и использовании шифровальных (криптографических) средств защиты информации».
7.	Организационно-штатные мероприятия обеспечения деятельности удостоверяющего центра.
8.	Регламент удостоверяющего центра (типы регламентов УЦ, основные положения типового регламента УЦ, дополнительные положения и документы).
9.	Работа с документами в организации (делопроизводство, документооборот, ГОСТ Р 6.30-2003, ГОСТ Р 51141-98, Типовая инструкция по делопроизводству в федеральных органах исполнительной власти).
10.	Доверие к открытому ключу и цифровые сертификаты (основные определения, стандарт X.509, сравнение версий сертификатов стандарта X.509, классы сертификатов, хранилище сертификатов в ОС Windows).
11.	Традиционные бумажные и электронные документы (аутентификация и корректность восприятия информации в бумажных и электронных документах, угрозы безопасности субъектам ЭД).
12.	Криптографические методы защиты информации (плюсы и минусы КМЗИ, симметричная и асимметричная криптография, сравнение, плюсы и минусы, комбинированный метод шифрования).
13.	Схема ЭЦП построенная на симметричной криптосистеме, схема ЭЦП построенная на асимметричной криптосистеме.

3.2 Вопросы к экзамену

ПК-2 - способностью создавать и исследовать модели автоматизированных систем

№ задания	Формулировка вопроса
1.	Основные определения Public Key Infrastructure (PKI)
2.	Криптопровайдеры входящие в стандартный состав Windows 2003 Server. КриптоПро CSP
3.	Внешнее устройство хранения ключевой информации eToken: линейка моделей, функциональная модель, составляющие безопасности eToken PRO
4.	Цели применения, компоненты и их функции, пользователи PKI
5.	Принципы доверия в PKI модели доверительных отношений, регулируемые доверительные отношения
6.	Проверка подлинности цифровых сертификатов в инфраструктуре Windows PKI - процедуры сличения, построение и обработка цепочки сертификатов
7.	КриптоПро OCSP Server и КриптоПро Revocation Provider (основные определения, назначение, характеристики).
8.	КриптоПро TSP Server (основные определения, назначение, характеристики) и усовершенствованная подпись КриптоПро (схема и формат усовершенствованной подписи, архивное хранение, технологические процедуры создания и проверки усовершенствованной ЭЦП).
9.	ЭЦП на основе удостоверяющего центра КриптоПро структура, состав и основные возможности УЦ КриптоПро, взаимодействие компонентов УЦ КриптоПро,
10.	Режим работы удостоверяющего центра
11.	Криптопровайдеры входящие в стандартный состав Windows 2007 Server.
12.	Линейка моделей, функциональная модель, составляющие безопасности eToken PRO, жизненный цикл eToken PRO, уровни доступа
13.	Public Key Infrastructure (PKI) (Основные определения, целипримененения, компоненты и их функции, пользователи PKI).
14.	Принципы доверия в PKI (модели доверительных отношений, регулируемые доверительные отношения, настройка регулируемых доверительных отношений).
15.	Проверка подлинности цифровых сертификатов в инфраструктуре Windows PKI (проверка

	подлинности цепочки сертификатов, списки аннулированных сертификатов CLR; риск, связанный с технологией CLR).
16.	КриптоПро OCSP Server и КриптоПро Revocation Provider (основные определения, назначение, характеристики).
17.	КриптоПро TSP Server (основные определения, назначение, характеристики) и усовершенствованная подпись КриптоПро (схема и формат усовершенствованной подписи, архивное хранение, технологические процедуры создания и проверки усовершенствованной ЭЦП).
18.	Система электронного документооборота (определение, назначение, экономический эффект, стандарты ISO серии 9000, ISO 15489, DoD 5015.2, примеры СЭД).
19.	Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи".
20.	Особенности юридического определения ЭЦП в РФ.
21.	Положение о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами.
22.	Доверие к открытому ключу и цифровые сертификаты (основные определения, стандарт X.509, сравнение версий сертификатов стандарта X.509, классы сертификатов, хранилище сертификатов в ОС Windows).
23.	Традиционные бумажные и электронные документы (аутентификация и корректность восприятия информации в бумажных и электронных документах, угрозы безопасности субъектам ЭД).
24.	Криптографические методы защиты информации (плюсы и минусы КМЗИ, симметричная и асимметричная криптография, сравнение, плюсы и минусы, комбинированный метод шифрования).
25.	Схема ЭЦП построенная на симметричной криптосистеме, схема ЭЦП построенная на асимметричной криптосистеме.

3.3 Контрольные вопросы к текущим опросам на практических работах

ПК-2 - способностью создавать и исследовать модели автоматизированных систем

№ задания	Формулировка вопроса
1.	Перечислите основные угрозы информации в компьютерных системах.
2.	Перечислите особенности защиты информации на узлах компьютерной сети.
3.	Перечислите системы обнаружения атак.
4.	Уязвимости TCP/IP протокола?
5.	Что такое МЭ?
6.	Каковы основные аспекты создания системы обнаружения атак.
7.	Сетевые сенсоры.
8.	Виртуальная частная сеть.
9.	Аутентификация и авторизация. Уязвимости аутентификации и авторизации.
10.	Классификация уязвимостей.
11.	Уязвимости платформы Windows.
12.	Классификация атак.
13.	Модель атаки. Этапы реализации атак.
14.	Что такое система обнаружения атак.
15.	Схема работы системы обнаружения.
16.	Признаки атак. Источники информации об атаках.
17.	Технологии и подходы к обнаружению атак.
18.	Анализ сетевого трафика.
19.	Анализ сервисов и портов.
20.	Системы анализа защищенности.
21.	Журнал регистрации, его назначение
22.	Обманные системы.

23.	Системы контроля целостности.
24.	Предварительный анализ. Критерии оценки.
25.	Размещение системы обнаружения атак.
26.	Каково назначение систем обнаружения атак?
27.	Каковы основные виды систем обнаружения атак?
28.	Каковы особенности использования систем обнаружения компьютерных атак?
29.	Назначение, основные виды, особенности использования. Слабости МЭ, и способы его обхода
30.	Назначение сетевых сенсоров
31.	Основные виды сетевых сенсоров
32.	Особенности использования сетевых сенсоров
33.	Назначения виртуальных частных сетей
34.	Каковы основные виды виртуальных частных сетей?
35.	Каковы особенности использования виртуальных частных сетей?
36.	Размещение сетевых сенсоров в коммутируемых сетях.
37.	Анализ журнала регистрации.
38.	Назначение обманных систем
39.	Каковы особенности использования обманных систем
40.	Особенности использования журнала регистрации

3.4 Домашнее задание

ПК-2 - способностью создавать и исследовать модели автоматизированных систем

№ задания	Формулировка задания
1	Создание электронно-цифровой подписи к порталу «Госуслуги»
2	Создание электронно-цифровой подписи к «Мой банк»
3	Создание электронно-цифровой подписи к порталу «Штрафы ГИБДД»
4	Создание электронно-цифровой подписи к порталу «Налоговая»
5	Создание электронно-цифровой подписи к порталу «Библиотека»
6	Создание электронно-цифровой подписи к порталу «Интернет-магазин»
7	Создание электронно-цифровой подписи к порталу «Салоны красоты»
8	Создание электронно-цифровой подписи к порталу «Справочные службы»
9	Создание электронно-цифровой подписи к порталу «Авиабилеты во все направления»
10	Создание электронно-цифровой подписи к порталу «Билеты ж.д. и авто»

3.5 Темы докладов

ПК-2 - способностью создавать и исследовать модели автоматизированных систем

№ задания	Формулировка задания
1.	Организационно-штатные мероприятия обеспечения деятельности удостоверяющего центра.
2.	Положение о лицензировании деятельности.
3.	Правовые вопросы применения ЭЦП и СКЗИ в Росси.
4.	eToken – персональное средство аутентификации и хранения данных.
5.	УЦ построенный на технологиях ViPNet.
6.	Положение об удостоверяющем центре организации.
7.	Регламент УЦ. Типы регламентов УЦ.
8.	Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи".
9.	Российские и зарубежные стандарты делопроизводства и документооборота

3.6 Контрольные вопросы к собеседованию при защите лабораторных работ

ПК-2 - способностью создавать и исследовать модели автоматизированных систем

№ задания	Формулировка задания

1	Как защитить сайт на IIS с помощью ssl туннеля? Отозвать сертификат в удостоверяющем центре и проверить, что пользователь не может зайти на сайт.
2	Как настроить аутентификацию пользователей по сертификату на этом сайте?
3	Как выдать пользователю сертификат, проверить, что пользователь с этим сертификатом заходит?
4	Как проверить есть у пользователя сертификата и зайдёт ли он?
	Как сертификаты раздаются при помощи УЦ?

3.7 Тематика курсовых работ

ПК-2 - способностью создавать и исследовать модели автоматизированных систем

Формулировка задания: Обеспечение правила разграничения доступа четырьмя функциями

Вар.	Обозначение		Уровни обеспечения защиты информации												
			I	II	III						IV				V
1	Функция		-	-	III.1		III.2		III.3	III.4	IV.1		IV.2	IV.3	-
	Мат.ожид.	A	1,50	1,50	3,00		4,00		2,00	1,00	0,30		0,30	5,00	7,00
	Ср.кв.откл.	B	-	-	0,50		8,00		5,00	0,50	0,50		0,50	1,50	-
	Зак.распр.	Z	Д	Д	Н		Р		Р	Н	Р		Р	Н	Д
	Вер.пер.	P	-	-	P(III)1,2	P(III)1,4	P(III)2,3	P(III)2,4	-	-	P(IV)1,2	P(IV)1,3	-	-	-
			-	-	0,50	0,50	0,50	0,50	-	-	0,50	0,50	-	-	-
Вар.	Обозначение		Уровни обеспечения защиты информации												
			I	II	III						IV				V
2	Функция		-	-	III.1		III.2		III.3	III.4	IV.1		IV.2	IV.3	-
	Мат.ожид.	A	-	1,50	3,00		4,00		2,00	1,00	0,30		0,30	5,00	7,00
	Ср.кв.откл.	B	-	-	0,50		8,00		5,00	0,50	0,50		0,50	1,50	-
	Зак.распр.	Z	-	Д	Н		Р		Р	Н	Р		Р	Н	Д
	Вер.пер.	P	-	-	P(III)1,2	P(III)1,4	P(III)2,3	P(III)2,4	-	-	P(IV)1,2	P(IV)1,3	-	-	-
			-	-	0,50	0,50	0,50	0,50	-	-	0,50	0,50	-	-	-
Вар.	Обозначение		Уровни обеспечения защиты информации												
			I	II	III						IV				V
3	Функция		-	-	III.1		III.2		III.3	III.4	I V.1		IV.2	IV.3	-
	Мат.ожид.	A	0,98	0,90	1,48		2,65		1,79	0,10	0,21		0,13	2,48	2,15
	Ср.кв.откл.	B	-	-	0,04		0,05		2,47	0,26	0,25		0,15	1,11	-
	Зак.распр.	Z	Д	Д	Н		Р		Н	Н	Н		Н	Н	Д
	Вер.пер.	P	-	-	P(III)1,2	P(III)1,4	P(III)2,3	P(III)2,4	-	-	P(IV)1,2	P(IV)1,3	-	-	-
			-	-	0,48	0,52	0,89	0,11	-	-	0,74	0,26	-	-	-
Вар.	Обозначение		Уровни обеспечения защиты информации												
			I	II	III						IV				V
4	Функция		-	-	III.1		III.2		III.3	III.4	IV.1		IV.2	IV.3	-
	Мат.ожид.	A	-	0,45	1,12		1,62		0,62	0,16	0,02		0,05	1,30	1,83
	Ср.кв.откл.	B	-	-			5,56		1,65	0,40				0,18	-
	Зак.распр.	Z	-	Д	Э		Р		Р	Р	Э		Э	Н	Д
	Вер.пер.	P	-	-	P(III)1,2	P(III)1,4	P(III)2,3	P(III)2,4	-	-	P(IV)1,2	P(IV)1,3	-	-	-
			-	-	0,90	0,10	0,53	0,47	-	-	0,86	0,14	-	-	-
Вар.	Обозначение		Уровни обеспечения защиты информации												
			I	II	III						IV				V
5	Функция		-	-	III.1		III.2		III.3	III.4	IV.1		IV.2	IV.3	-
	Мат.ожид.	A	1,71	1,12	1,13		3,18		2,39	1,04	1,07		1,05	3,32	2,71
	Ср.кв.откл.	B	-	-						1,07	1,23		1,00		-
	Зак.распр.	Z	Д	Д	Э		Э		Э	Р	Н		Н	Э	Д
	Вер.пер.	P	-	-	P(III)1,2	P(III)1,4	P(III)2,3	P(III)2,4	-	-	P(IV)1,2	P(IV)1,3	-	-	-
			-	-	0,76	0,24	0,69	0,31	-	-	0,74	0,26	-	-	-
Вар.	Обозначение		Уровни обеспечения защиты информации												

			I	II	III						IV				V
6	Функция		-	-	III.1		III.2		III.3	III.4	IV.1		IV.2	IV.3	-
	Мат.ожид.	A	-	1,37	1,41		1,04		1,09	1,11	1,00		1,02	2,09	2,78
	Ср.кв.откл.	B	-	-					1,77	1,19			1,28		-
	Зак.распр.	Z	-	Д	Э		Э		Р	Н	Э		Р	Э	Д
	Вер.пер.	P	-	-	P(III)1,2	P(III)1,4	P(III)2,3	P(III)2,4	-	-	P(IV)1,2	P(IV)1,3	-	-	-
			-	-	0,92	0,08	0,12	0,88	-	-	0,08	0,92	-	-	-

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

Процедуры оценивания в ходе изучения дисциплины знаний, умений и навыков, характеризующих этапы формирования компетенций, регламентируются положениями:

- П ВГУИТ 2.4.03 – 2015 Положение о курсовых, экзаменах и зачетах;
- П ВГУИТ 4.1.02 – 2012 Положение о рейтинговой оценке текущей успеваемости.

Итоговая оценка по дисциплине определяется на основании определения средневзвешенному значения баллов по каждому заданию.

5. Описание показателей и критериев оценивания уровня сформированности компетенций

Результаты обучения по этапам формирования компетенций	Методика оценки (объект, продукт или процесс)	Показатель оценивания	Критерии оценивания сформированности компетенций	Шкала оценивания	
				Академическая оценка или баллы	Уровень освоения компетенции
ПК-2 - способностью создавать и исследовать модели автоматизированных систем					
ЗНАТЬ: современные системы электронного документооборота	Экзамен	Уровень владения материалом	ответил на все вопросы, допустил не более 1 ошибки в ответе	Отлично	Освоена (повышенный)
			ответил на все вопросы, допустил более 1, но менее 3 ошибок	Хорошо	Освоена (повышенный)
			ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки	Удовлетворительно	Освоена (базовый)
			ответил не на все вопросы, допустил более 5 ошибок	Неудовлетворительно	Не освоена (недостаточный)
	Зачет	Уровень владения материалом	ответил на все вопросы, допустил не более 1 ошибки в ответе	Зачтено	Освоена (повышенный, базовый)
			ответил не на все вопросы, допустил более 5 ошибок	Не зачтено	Освоена (недостаточный)
УМЕТЬ: практически выполнять технологические операции по защите и обработке документов в системах электронного документооборота	Контрольные вопросы к текущим опросам на лабораторных работах	Уровень умения	студент выполнил задание и ответил на все вопросы и допустил не более 1 ошибки в ответе	Отлично	Освоена (повышенный)
			студент выполнил задание и ответил на все вопросы и допустил более 1 ошибки, но менее 3 ошибок	Хорошо	Освоена (повышенный)
			студент выполнил задание не полностью и ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки	Удовлетворительно	Освоена (базовый)
			студент ответил не на все вопросы, допустил более 5 ошибок	Неудовлетворительно	Не освоена (недостаточный)
ВЛАДЕТЬ: методами управления электронного документооборота	Курсовая работа	Уровень работы, презентации, доклада, оформ-	выставляется студенту при наличии курсовой работы, преобразовании информации в единую форму, презентации по выбранной теме, использованием не менее 10 источников, высоким уровнем владения представляемой информации	Отлично	Освоена (повышенный)

		ления	выставляется студенту при наличии курсовой работы, преобразовании информации в единую форму, презентации по выбранной теме, использованием менее 10 источников, низким уровнем владения представляемой информации	Хорошо	Освоена (повышенный)
			выставляется студенту при наличии доклада, презентации по выбранной теме, использованием менее 10 источников, не раскрытием поставленной задачи, наличием ошибок в расчетах	Удовлетворительно	Освоена (базовый)
			выставляется студенту при наличии информации только из одного источника, и (или) отсутствии презентации по выбранной теме	Не удовлетворительно	Не освоена (недостаточный)
	Домашняя работа	Уровень навыков	студент выбрал верную методику решения задач, ответил на все вопросы, допустил не более 1 ошибки в ответе	Отлично	Освоена (повышенный)
			студент выбрал верную методику решения задач, проведен верный расчет ответил на все вопросы, имеются незначительные замечания по тексту и оформлению работы, допустил не более 3 ошибок в ответе	Хорошо	Освоена (повышенный)
			студент выбрал верную методику решения задач, проведен верный расчет, представил решение задач, ответил на все вопросы, имеются значительные замечания по тексту и оформлению работы, допустил не более 5 ошибок в ответе	Удовлетворительно	Освоена (базовый)
			студент выбрал верную методику решения задач, проведен верный расчет, выполнил правильно графическую часть, представил решение задач, ответил на все вопросы, имеются значительные замечания по тексту и оформлению работы, допустил более 5 ошибок в ответе	Не удовлетворительно	Не освоена (недостаточный)

	Доклад	Уровень знаний	выставляется студенту при наличии доклада, преобразовании информации в единую форму, презентации по выбранной теме, использованием не менее 10 источников, высоким уровнем владения представляемой информации	Отлично	Освоена (повышенный)
			выставляется студенту при наличии доклада, преобразовании информации в единую форму, презентации по выбранной теме, использованием менее 10 источников, низким уровнем владения представляемой информации	Хорошо	Освоена (повышенный)
			выставляется студенту при наличии доклада, презентации по выбранной теме, использованием менее 10 источников, не раскрытием поставленной задачи	Удовлетворительно	Освоена (базовый)
			выставляется студенту при наличии информации только из одного источника, и (или) отсутствии презентации по выбранной теме	Не удовлетворительно	Не освоена (недостаточный)