

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

УТВЕРЖДАЮ
Проректор по учебной работе

(подпись)

Василенко В.Н.
(Ф.И.О.)

«26» мая 2022

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Технологии разработки защищенного документооборота

Специальность

10.05.03 Информационная безопасность автоматизированных систем

Специализация

Безопасность открытых информационных систем

Квалификация (степень) выпускника

специалист по защите информации

Разработчик _____
(подпись) (дата) (Ф.И.О.)

СОГЛАСОВАНО:

Заведующий кафедрой _____ информационной безопасности _____
(наименование кафедры, являющейся ответственной за данное направление подготовки, профиль)

_____ Скрыпников А.В. _____
(подпись) (дата) (Ф.И.О.)

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 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 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, программными 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, хранения 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 автоматизированным системам обработки и хранения электронных документов;	навыками работы с информационными системами электронного документооборота
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 и систем обеспечения информационной 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:

- Мультимедиа технологии;
- 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
<i>в том числе в форме практической подготовки</i>	–	–	–
Лабораторные работы (ЛР)	30	–	30
<i>в том числе в форме практической подготовки</i>	–	–	–
Практические занятия (ПЗ)	66	36	30
<i>в том числе в форме практической подготовки</i>	–	–	–
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

5.2.1 Лекции

№ 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 MakeCert 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 сертификата 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 certificate 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

5.2.4 Самостоятельная 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		2
7	Электронные сертификаты		6
8	CryptoAPI и криптопровайдеры	Курсовая работа	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.vsu.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. Данылиев, 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;
--	---	--

	<p>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 SHS-2920; средство активной защиты информации изделие «Салют 2000С» с регулятором выходного уровня шума</p>	<p>Sublime Text; Symantec Endpoint Protection 12 (Заменен на AVP Kaspersky); VMWare Player; Антивирус "Зоркий глаз"; Lazarus; SmathStudio; NanoCAD; Gimp (графический редактор, аналог Photoshop); Avidemux (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</p>
<p>Аудитории для проведения занятий лекционного типа, лабораторных и практических занятий</p>	<p>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-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 SHS-2920</p>	<p>Ауд.332а: OC 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: OC 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;</p>

		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.

**АННОТАЦИЯ
К РАБОЧЕЙ ПРОГРАММЕ
ДИСЦИПЛИНЫ
«ТЕХНОЛОГИЯ РАЗРАБОТКИ ЗАЩИЩЕННОГО ДОКУМЕНТООБОРОТА»**
(наименование дисциплины)

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2);
- способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);
- 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 (ОК-5);
- способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах (ОПК-4);
- способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-5);
- способностью применять нормативные правовые акты в профессиональной деятельности (ОПК-6);
- способностью создавать и исследовать модели автоматизированных систем (ПК-2);
- способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);
- способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);
- способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);
- способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21).

В результате освоения дисциплины студент должен:

Знать

- о современных направлениях развития и совершенствования процессов управления экономическими, социальными и производственными процессами в организационных структурах различных типов и форм собственности;
- правовые основы защиты конфиденциальной информации по видам тайны; правовые основы деятельности подразделений защиты информации; порядок лицензирования деятельности по технической защите конфиденциальной информации;
- 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;
- тенденции развития информационных технологий, необходимых для поиска информации в компьютерных системах, сетях, библиотечных фондах;
- правовые нормы в области защиты интеллектуальной собственности;
- организацию работы руководителей, специалистов и технического персонала с конфиденциальными документами на любом носителе информации;
- современные системы электронного документооборота, основные тенденции развития автоматизированных систем и способов обработки и хранения конфиденциальных документов, а также совершенствования носителей документной информации;
- 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;

- организацию конфиденциального документооборота; технологию работы с конфиденциальными документами; организацию электронного документооборота;
- существующие типы автоматизированных систем и способы обработки и хранения конфиденциальных документов, функциональные возможности этих систем, номенклатуре вычислительной и организационной техники;
- основы разработки программ и методик испытаний средств и систем обеспечения информационной безопасности;

Уметь

- организовывать работу руководителей, специалистов и технического персонала с документами в системах электронного документооборота;
- использовать в профессиональной деятельности 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;
- применять полученные знания и навыки в своей дальнейшей профессиональной деятельности;
- использовать современные защищенные информационные технологии для поиска информации в компьютерных системах, сетях, библиотечных фондах;
- разрабатывать эффективные технологические схемы рационального документооборота с использованием современных систем и способов обработки и хранения конфиденциальных документов;
- руководить службой конфиденциальной документации;
- практически выполнять технологические операции по защите и обработке документов в системах электронного документооборота;
- разрабатывать и оформлять нормативно-методические материалы по регламентации процессов обработки, хранения и защиты конфиденциальных документов;
- определять состав документированной конфиденциальной информации; подготавливать, издавать и учитывать конфиденциальные документы;
- формулировать задачи по разработке потребительских требований к автоматизированным системам обработки и хранения электронных документов;
- разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации;

Владеть

- владеть современными технологиями управления персоналом;
- методиками модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России. ФСТЭК России;
- навыками создания и использования систем электронного документооборота и организации их защиты;
- навыками использования новейших информационных технологий; передового отечественного и зарубежного опыта по разработке автоматизированных систем управления технологическими процессами, программными средствами визуального представления;
- обработкой и сравнительным анализом справочной и реферативной информации;
- навыками организации работы малых коллективов исполнителей по защите электронной документации;
- методами управления электронного документооборота;
- способностью к контролю соответствия разрабатываемых проектов и технической документации стандартам, техническим условиям и другим нормативным документам;
- способностью к разработке проектной и рабочей технической документации, оформлению законченных проектных работ в соответствии с нормами и стандартами;
- навыками работы с информационными системами электронного документооборота;
- способностью к разработке программ и методик испытаний средств и систем обеспечения информационной безопасности.

Содержание разделов дисциплины. Основные понятия и определения электронного документооборота. Федеральный закон об электронной подписи. Работа с документами в организации. “Электронная революция” в работе с документами. Особенности рынка систем управления деловыми процессами. Составляющие экономического эффекта. Стандарты ISO серии 9000. Стандарт ISO15489. DoD 5015.2. Документ на бумажном носителе и рукописная подпись. Электронные документы. Важнейшие реквизиты электронного документооборота. Угрозы безопасности субъектам электронного документооборота. Определение и функции электронно-цифровой подписи. 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. Определение электронных сертификатов. Сертификаты X.509. Классы сертификатов. Хранилища сертификатов. Импорт и экспорт сертификатов. Архитектура CryptoAPI. Определение и функции криптопровайдера. 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. Определение и цели применения PKI. Компоненты PKI. Принципы доверия PKI. Назначение и характеристики КриптоПро OCSP Server. КриптоПро Revocation Provider. Назначение КриптоПро TSP Server. Схема усовершенствованной подписи КриптоПро. Технологические процедуры. Создание усовершенствованной электронной цифровой подписи. Основные возможности, назначение и применение «Удостоверяющего Центра КриптоПро УЦ». Формат и состав сертификатов, поддерживаемых «КриптоПро УЦ». Основные расширения CLR