МИНОБРНАУКИ РОССИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»

(БГТУ им. В.Г. Шухова)

СОГЛАСОВАНО
Директор института
заочного образования
«20» 05 2021 г.

УТВЕРЖДАЮ
Директор института ЭИТУС
А.В. Белоусов
«20» 05 2021 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

Информационная безопасность

направление подготовки

09.03.02 Информационные системы и технологии

Направленность программы

Информационные системы и технологии

Квалификация

бакалавр

Форма обучения

заочная

Институт: Энергетики, информационных технологий и управляющих систем

Кафедра: Информационных технологий

Белгород 2021

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению 09.03.02 Информационные системы и технологии, утвержденного Приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. № 926
- учебного плана, утвержденного ученым советом БГТУ им. В.Г. Шухова в 2021 году.

Составитель: ст.преп. _____ (С.И.Жданова)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа обсуждена на заседании кафедры

«30» 04 2021 г., протокол № 6

И.о. зав. кафедрой: канд.техн.наук _____ (Д.Н. Старченко)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа согласована с выпускающей кафедрой
информационных технологий

И.о. зав. кафедрой: канд.техн.наук _____ (Д.Н. Старченко)
(ученая степень и звание, подпись) (инициалы, фамилия)

«30» 04 2021 г.

Рабочая программа одобрена методической комиссией института

«20» 05 2021 г., протокол № 9

Председатель: канд.техн.наук, доц. _____ (А.Н. Семернин)
(ученая степень и звание, подпись) (инициалы, фамилия)

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Категория (группа) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Наименование показателя оценивания результата обучения по дисциплине
	УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.	УК-2.1. Определяет круг актов действующего законодательства, содержащих правовые нормы, регулирующие профессиональную деятельность	Знание основных категории и аспектов информационной безопасности; основных законодательных, процедурных, административных и программно-технических мер обеспечения информационной безопасности;
		УК-2.2. Использует нормативно-правовые документы при разработке и реализации профессиональных проектов	Умение организовать процесс защиты информационных систем в соответствии с отечественными и международными стандартами в области информационной безопасности;
		УК-2.3. Осуществляет составление договоров и других правовых документов, использует информационно-правовые ресурсы для решения профессиональных задач, соблюдая при этом требования антикоррупционного законодательства	Владение навыками составления договоров и других нормативно-правовых документов с использованием информационно-правовых ресурсов для решения профессиональных задач, с соблюдением требования антикоррупционного законодательства.
	ОПК-2. Способен использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	ОПК-2.1. Понимает принципы работы современных информационных технологий и программных средств.	Знание содержания основных отечественных и международных стандартов и спецификаций, действующих в области информационной безопасности;
		ОПК-2.2. Использует современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	Умение определить уязвимые места в защите информационной системы, выбрать необходимые и экономически обоснованные защитные мероприятия на административном, процедурном и программно-техническом уровнях обеспечения безопасности;
		ОПК-2.3. Осуществляет выбор современных информационных	Владение навыками применения криптографических пакетов и интерфейсов для построения подсистем информационной

		технологий и программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности	безопасности.
	ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Использует принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знание основ построения криптосистем, а также средств создания и верификации электронных подписей и аутентификации; особенности защиты распределенных информационных систем
		ОПК-3.2. Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	Умение осуществлять программную реализацию наиболее распространенных крипто алгоритмов, применять существующие системы защиты от несанкционированного доступа.
		ОПК-3.3. Подготавливает обзоры, аннотации, составляет рефераты, научные доклады, публикации и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Владение моделями, стратегиями систем и технологических основ комплексного обеспечения информационной безопасности, вопросами правового и организационного обеспечения информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1. Компетенция УК-2

Данная компетенция формируется следующими дисциплинами.

Стадия	Наименования дисциплины
1	Социология и психология
2	Правоведение
3	Основы экономики
4	Управление IT проектами
5	Информационная безопасность
6	Стандартизация и лицензирование ПО
7	Научно-техническая информация

2. Компетенция ОПК-2

Данная компетенция формируется следующими дисциплинами.

Стадия	Наименования дисциплины
1	Информационные технологии
2	Управление данными
3	Большие данные
4	Инструментальные средства информационных систем
5	Интеллектуальные системы и технологии
6	Информационная безопасность
7	Программная инженерия
8	Технология обработки информации
9	Учебная технологическая (проектно-технологическая) практика

3. Компетенция ОПК-3

Данная компетенция формируется следующими дисциплинами.

Стадия	Наименования дисциплины
1	Управление данными
2	Администрирование информационных систем
3	Инфокоммуникационные системы и сети
4	Управление IT-проектами
5	Информационная безопасность
6	Учебная ознакомительная практика
7	Учебная технологическая (проектно-технологическая) практика

3. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 5 зач. единиц, 180 часов.

Форма промежуточной аттестации экзамен

(экзамен, дифференцированный зачет, зачет)

Вид учебной работы	Всего часов	Семестр № 7	Семестр № 8
Общая трудоемкость дисциплины, час	180	3	177
Контактная работа (аудиторные занятия), в т.ч.:	10	2	8
лекции	4	2	2
лабораторные	4		4
практические			
групповые консультации в период теоретического обучения и промежуточной аттестации	2		2
Самостоятельная работа студентов, включая индивидуальные и групповые консультации, в том числе:	170	1	169
Курсовой проект			
Курсовая работа			
Расчетно-графическое задание			
Индивидуальное домашнее задание	9		9
Самостоятельная работа на подготовку к аудиторным занятиям (лекции, практические занятия, лабораторные занятия)		1	124
Экзамен	36		36

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Наименование тем, их содержание и объем
Курс 4 Семестр 7

№ п/п	Наименование раздела (краткое содержание)	Объем на тематический раздел по видам учебной нагрузки, час			
		Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа на подготовку к аудиторным занятиям
1.	Раздел 1. Основные аспекты информационной безопасности				
	Понятие информационной безопасности. Основные категории информационной безопасности. Законодательные аспекты информационной безопасности. Анализ наиболее распространенных угроз и методов проникновения в информационные системы. Программное обеспечение, применяемое для проникновения в информационные системы и методы нейтрализации его воздействия.	1			0,5
2.	Раздел 2. Криптографические средства защиты информации				
	Основные понятия криптографии, терминология. Классификация криптоалгоритмов. Основные виды криптоаналитических атак. Законодательство РФ в области разработки и применения систем, содержащих элементы криптозащиты. Потоковые и блочные шифры. Принципы построения блочных шифров. Конструкции Фейстеля. Режимы работы блочных шифров. Криптоалгоритмы AES, ГОСТ 28147-89 и ГОСТ Р 34.12-2015. Основные принципы шифрования с открытым ключом. Области применения криптосистем с открытым ключом. Криптоалгоритм RSA. Управление ключами. Алгоритм Диффи-Хеллмана-Меркла.	1			0,5
	ВСЕГО	2			1

Курс 4 Семестр 8

№ п/п	Наименование раздела (краткое содержание)	Объем на тематический раздел по видам учебной нагрузки, час			
		Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа на подготовку к аудиторным занятиям
3.	Раздел 3. Стандарты информационной безопасности				

	Основные понятия, вводимые стандартами и спецификациями. Руководящие документы Гостехкомиссии РФ. Нормативные документы ФСТЭК. Обзор наиболее значимых отечественных стандартов в области информационной безопасности: ИСО/МЭК 15408, серия стандартов ИСО/МЭК 27000.	0,4		0,57	18,7
4.	Раздел 4. Электронная подпись и аутентификация				
	Назначение функций хэширования и предъявляемые к ним требования. Обзор известных алгоритмов хэширования: MD5, SHA-1, 2, 3, ГОСТ Р 34.11-94, 2012. Требования к электронным подписям. Основные положения закона 63-ФЗ «Об электронной подписи». Характеристики алгоритмов создания и верификации электронных подписей: DSA, ECDSA, ГОСТ Р 34.10-94, 2001, 2012. Протоколы односторонней и двусторонней аутентификации на основе симметричного и асимметричного шифрования. Основные положения стандарта X.509. Структура сертификата открытого ключа, форматы хранения. Отзыв сертификатов. Общая схема аутентификации с использованием сертификатов X.509. Инфраструктуры открытых ключей.	0,4		0,57	18,7
5.	Раздел 5. Защита распределенных систем и корпоративных сетей				
	Особенности протоколов защищенного обмена данными сетевого и транспортного уровня и их место в стеке протоколов TCP/IP. Обзор защищенных протоколов: IPSec, SSL, TLS. Атакуемые сетевые компоненты информационных систем. Классификация нарушителей сетевой безопасности информационных систем. Управление доступом. Методика обнаружения нарушителей. Протоколирование и аудит. Классификация вредоносных программ. Антивирусная защита. Основные характеристики и типы брандмауэров и систем обнаружения и предотвращения вторжений.	0,4		0,57	18,7
6.	Раздел 6. Системы защиты электронной почты				
	Назначение и принцип работы систем PGP и S/MIME.	0,4		0,57	18,7
7.	Раздел 7. Организационное обеспечение информационной безопасности				
	Административный уровень информационной безопасности. Формирование политики безопасности. Управление рисками. Процедурный уровень информационной безопасности. Основные меры поддержания работоспособности информационной системы.	0,4		0,57	18,7
	ВСЕГО	2		4	124

4.2. Содержание практических (семинарских) занятий

Не предусмотрено учебным планом

4.3. Содержание лабораторных занятий

№ п/п	Наименование раздела дисциплины	Тема лабораторного занятия	К-во часов	Самостоятельная работа на подготовку к аудиторным занятиям
семестр № 6				
1	Криптографические средства защиты информации	Потоковое шифрование данных	0,67	20,3
2		Алгоритм блочного шифрования данных ГОСТ 28147-89	0,67	20,3
3		Симметричное шифрование данных с использованием криптографических интерфейсов Microsoft CryptoAPI и Cryptography API: Next Generation	0,67	20,3
4		Симметричное и асимметричное шифрование данных средствами криптографического пакета OpenSSL	0,67	20,3
5	Электронная подпись и аутентификация	Создание криптографических сообщений с использованием интерфейса Microsoft CryptoAPI и цифровых сертификатов X.509	0,67	20,3
6	Защита распределенных систем и корпоративных сетей	Реализация защищенной передачи данных по протоколу TLS средствами криптографического пакета OpenSSL	0,67	20,3
		ИТОГО:	4	122
			ВСЕГО:	126

4.4. Содержание курсового проекта/работы

Не предусмотрено учебным планом

4.5. Содержание расчетно-графического задания, индивидуальных домашних заданий

Не предусмотрено учебным планом

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5.1. Реализация компетенций

1 Компетенция УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Наименование индикатора достижения компетенции	Используемые средства оценивания
УК-2.1. Определяет круг актов действующего законодательства, содержащих правовые нормы, регулирующие профессиональную деятельность.	Собеседование, защита лабораторной работы, тестовый контроль, устный опрос, экзамен
УК-2.2. Использует нормативно-правовые документы при разработке и реализации профессиональных проектов.	Собеседование, защита лабораторной работы, тестовый контроль, устный опрос, экзамен
УК-2.3. Осуществляет составление договоров и других правовых документов, использует информационно-правовые ресурсы для решения профессиональных задач, соблюдая при этом требования антикоррупционного законодательства	Собеседование, защита лабораторной работы, тестовый контроль, устный опрос, экзамен

2 Компетенция ОПК-2. Способен использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности

Наименование индикатора достижения компетенции	Используемые средства оценивания
ОПК-2.1. Понимает принципы работы современных информационных технологий и программных средств.	Собеседование, защита лабораторной работы, тестовый контроль, устный опрос, экзамен
ОПК-2.2. Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности.	Собеседование, защита лабораторной работы, тестовый контроль, устный опрос, экзамен
ОПК-2.3. Осуществляет выбор современных информационных технологий и программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности	Собеседование, защита лабораторной работы, тестовый контроль, устный опрос, экзамен

3 Компетенция ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной

безопасности

Наименование индикатора достижения компетенции	Используемые средства оценивания
ОПК-3.1. Использует принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Собеседование, защита лабораторной работы, тестовый контроль, устный опрос, экзамен
ОПК-3.2. Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Собеседование, защита лабораторной работы, тестовый контроль, устный опрос, экзамен
ОПК-3.3. Подготавливает обзоры, аннотации, составляет рефераты, научные доклады, публикации и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Собеседование, защита лабораторной работы, тестовый контроль, устный опрос, экзамен

5.2. Типовые контрольные задания для промежуточной аттестации

5.2.1. Перечень контрольных вопросов (типовых заданий) для экзамена / дифференцированного зачета / зачета

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1	Основные аспекты информационной безопасности	Понятие информационной безопасности. Основные типы угроз информационной безопасности
2		Законодательные аспекты информационной безопасности.
3	Криптографические средства защиты информации	Базовые понятия криптографии. Основные задачи, решаемые с помощью криптографии. Понятия криптоалгоритма и ключа
4		Криптоанализ. Понятие стойкости алгоритма. Основные разновидности криптоаналитических атак
5		Классификация алгоритмов классической криптографии. Одноразовые блокноты. Классификация компьютерных криптоалгоритмов.
6		Принципы построения блочных шифров. Сеть Фейстеля
7		Основные режимы работы блочных шифров
8		Криптоалгоритм ГОСТ 28147-89. Структура раунда. Базовые циклы зашифрования и расшифрования. Режимы шифрования, определенные стандартом
9		Криптоалгоритм AES. Характеристики алгоритма и его структура
10		Криптосистемы с открытым ключом. Принципы построения

		и отличия от симметричных криптосистем. Алгоритм с открытым ключом RSA
11		Управление ключами в симметричных и асимметричных криптосистемах. Генерация ключей. Распределение ключей для симметричных криптосистем
12		Обмен сеансовыми ключами средствами симметричной криптографии и криптографии с открытым ключом. Способы хранения ключей. Время жизни ключей
13		Алгоритм обмена ключами Диффи-Хеллмана-Меркла.
14		Потоковые шифры A5 и RC4
15	Стандарты информационной безопасности	Стандарты информационной безопасности РФ
16	Электронная подпись и аутентификация	Однонаправленные хэш-функции. Назначение. Основные требования, предъявляемые к хэш-функциям. Коллизии и их использование в процессе подделки сообщений
17		Характеристики и общие принципы построения алгоритмов хэширования MD5, SHA-1, 2, 3, ГОСТ Р 34.11-94, 2012
18		Коды проверки подлинности сообщений (MAC)
19		Электронная подпись (ЭП). Назначение электронной подписи, ее виды. Требования к ЭП. Общие принципы создания ЭП. Стандарты ЭП РФ и США
20		Протоколы односторонней и двухсторонней аутентификации
21		Стандарт X.509. Структура сертификата разных версий. Форматы хранения сертификатов
22		Стандарт X.509. Принципы аутентификации. Отзыв сертификатов
23		Инфраструктуры открытых ключей
24	Защита распределенных систем и корпоративных сетей	Атакуемые сетевые компоненты информационных систем. Классификация нарушителей сетевой безопасности информационных систем
25		Основные характеристики и типы брандмауэров и систем обнаружения и предотвращения вторжений
26		Защищенный протокол передачи данных IPSec
27		Защищенный протокол передачи данных SSL/TLS
28	Системы защиты электронной почты	Система защиты электронной почты PGP
29		Система защиты электронной почты S/MIME
30	Организационное обеспечение информационной безопасности	Организационное обеспечение информационной безопасности

5.2.2. Перечень контрольных материалов для защиты курсового проекта/ курсовой работы

Не предусмотрено учебным планом

5.3. Типовые контрольные задания (материалы) для текущего контроля в семестре

Контроль знаний студентов осуществляется в процессе выполнения и защиты лабораторных работ, а также сдачи экзамена.

"Выполнение" лабораторной работы предполагает демонстрацию студентом результатов выполнения заданий, а именно отчета и необходимых файлов. Полные перечни заданий с примерами выполнения приведены в методических указаниях по выполнению лабораторных работ по дисциплине "Информационная безопасность".

Примерные варианты заданий приведены в следующей таблице.

	Тема лабораторной работы	Задание
	Семестр 6. Лабораторная работа №1. Потоковое шифрование данных	Получить навыки в создании программной реализации алгоритма потокового шифрования на базе регистра сдвига с линейной обратной связью.
	Семестр 6. Лабораторная работа №2. Алгоритм блочного шифрования данных ГОСТ 28147-89.	Научиться реализовывать на выбранном языке программирования алгоритм блочного шифрования данных ГОСТ 28147-89
	Семестр 6. Лабораторная работа №3. Симметричное шифрование данных с использованием криптографических интерфейсов Microsoft CryptoAPI и Cryptography API: Next Generation	Ознакомиться с понятием криптопровайдера в интерфейсе CryptoAPI и провайдера алгоритма в интерфейсе Cryptography API: Next Generation, способами подключения к ним, получить навыки выполнения базовых криптографических преобразований: хэширования и симметричного шифрования.
	Семестр 6. Лабораторная работа №4. Симметричное и асимметричное шифрование данных средствами криптографического пакета OpenSSL	Ознакомиться со средствами симметричного и асимметричного шифрования, предоставляемыми пакетом OpenSSL и способами доступа к ним из приложений на языке C/C++.
	Семестр 6. Лабораторная работа	Ознакомиться со структурой и форматами представления сертификатов открытых ключей,

	Тема лабораторной работы	Задание
	№5. Создание криптографических сообщений с использованием интерфейса Microsoft CryptoAPI и цифровых сертификатов X.509.	способами их создания и импортирования в систему, а также получить навыки в создании криптографических сообщений средствами интерфейса Microsoft CryptoAPI..
	Семестр 6. Лабораторная работа №6. Реализация защищенной передачи данных по протоколу TLS средствами криптографического пакета OpenSSL.	Ознакомиться со способами организации защищенных TLS-соединений средствами криптографического пакета OpenSSL, а также получить навыки в создании простейших клиентских и серверных приложений в среде Visual Studio.

В процессе демонстрации результатов студенту может быть предложено ответить на несколько вопросов, связанных с тематикой работы. Примерный перечень вопросов приведен в следующей таблице.

	Тема лабораторной работы	Контрольные вопросы
	Семестр 6. Лабораторная работа №1. Потоковое шифрование данных	1. Принципы работы потоковых шифров. 2. Какие операции используются при реализации потоковых шифров? 3. Что такое гамма шифра? 4. Что представляет собой регистр сдвига с линейной обратной связью? 5. Что такое отводная последовательность, и в какой форме ее можно представить??
	Семестр 6. Лабораторная работа №2. Алгоритм блочного шифрования данных ГОСТ 28147-89.	1. Что такое сеть Фейстеля? Каковы основные принципы работы блочных шифров, устроенных по принципу сети Фейстеля? 2. Назовите все режимы шифрования, определенные в ГОСТ 28147-89. 3. Каковы разрядности блока и ключа в алгоритме ГОСТ 28147- 89? 4. Что представляют собой таблицы замен (S-блоки) в алгоритме ГОСТ 28147-89? 5. Что представляет собой один раунд (основной шаг) алгоритма ГОСТ 28147-89?
	Семестр 6. Лабораторная работа	1. Что такое CryptoAPI? В чем заключается различие между CryptoAPI 1.0 и CryptoAPI 2.0?

	Тема лабораторной работы	Контрольные вопросы
	№3. Симметричное шифрование данных с использованием криптографических интерфейсов Microsoft CryptoAPI и Cryptography API: Next Generation	2. Что такое криптопровайдер? Как можно подключиться к криптопровайдеру? 3. Какое количество функций должен поддерживать криптопровайдер? 4. Как создать контейнер ключей? Какие типы ключей в нем будут храниться? 5. Какие типы криптопровайдеров вы знаете? Чем они различаются?
	Семестр 6. Лабораторная работа №4. Симметричное и асимметричное шифрование данных средствами криптографического пакета OpenSSL	1. Для чего используется криптографический пакет OpenSSL? 2. В каких операционных системах можно использовать пакет OpenSSL? 3. Как установить и сконфигурировать пакет OpenSSL. 4. Как выполняется инициализация библиотеки шифрования? 5. Какие статические и динамические библиотеки пакета OpenSSL задействуются в данной работе?
	Семестр 6. Лабораторная работа №5. Создание криптографических сообщений с использованием интерфейса Microsoft CryptoAPI и цифровых сертификатов X.509.	1. Для чего используются сертификаты открытых ключей X.509? 2. Что такое инфраструктура открытых ключей (PKI)? Какие варианты архитектуры PKI вы знаете? 3. Какова структура сертификата X.509? 4. Как сертификаты X.509 хранятся в запоминающих устройствах? Какие форматы сертификатов вы знаете? 5. Что такое поля расширений в составе сертификата X.509?
	Семестр 6. Лабораторная работа №6. Реализация защищенной передачи данных по протоколу TLS средствами криптографического пакета OpenSSL.	1. Как в протоколе TLS осуществляется аутентификация сервера и клиента? 2. Как с помощью криптографического пакета OpenSSL осуществить генерацию ключевой пары алгоритма ГОСТ 34.10-2001 и создание самоподписанного сертификата? 3. Что собой представляет обобщенный алгоритм работы клиентского приложения, передающего и принимающего данные по протоколу TLS? 4. Какие функции WinSock API используются для открытия и закрытия сокетов, создания и разрыва TCP-соединений? 5. Как для клиентского приложения установить параметры хранилища доверенных сертификатов?

Процедура "выполнения" работ представляет собой качественную оценку знаний, умений и навыков студентов.

Количественная оценка предусматривается в процессе "защиты" работ, а также сдачи экзамена.

5.4. Описание критериев оценивания компетенций и шкалы оценивания

При промежуточной аттестации в форме экзамена, дифференцированного зачета, дифференцированного зачета при защите курсового проекта/работы используется следующая шкала оценивания: 2 – неудовлетворительно, 3 – удовлетворительно, 4 – хорошо, 5 – отлично.

Критериями оценивания достижений показателей являются:

Наименование показателя оценивания результата обучения по дисциплине	Критерий оценивания
Знание основных категории и аспектов информационной безопасности; основных законодательных, процедурных, административных и программно-технических мер обеспечения информационной безопасности;	Знание терминов, определений, понятий: основными категориями и аспектами информационной безопасности; основными законодательными, процедурными, административными и программно-техническими мерами обеспечения информационной безопасности.
	Знание основных закономерностей, соотношений, принципов
	Объем освоенного материала
	Полнота ответов на вопросы
	Четкость изложения и интерпретации знаний
Умение организовать процесс защиты информационных систем в соответствии с отечественными и международными стандартами в области информационной безопасности;	Освоение методик -умение решать практические задачи, выполнять типовые задания: защита информационных систем в соответствии с отечественными и международными стандартами в области информационной безопасности.
	Умение использовать теоретические знания для выбора методики решения задач, выполнения заданий
	Умение проверять решение и анализировать результаты
	Умение качественно оформлять (презентовать) решение задач и выполнения заданий
Владение навыками составления договоров и других нормативно-правовых документов с использованием информационно-правовых ресурсов для решения профессиональных задач, с соблюдением требования антикоррупционного	Навыки решения стандартных/нестандартных задач: криптографических алгоритмов для решения задач в области защиты информации.
	Объём выполненных заданий
	Качество выполнения трудовых действий
	Самостоятельность планирования выполнения трудовых действий

законодательства.	
Знание содержания основных отечественных и международных стандартов и спецификаций, действующих в области информационной безопасности;	Знание терминов, определений, понятий: содержание основных отечественных и международных стандартов и спецификаций, действующих в области информационной безопасности.
	Знание основных закономерностей, соотношений, принципов
	Объем освоенного материала
	Полнота ответов на вопросы
	Четкость изложения и интерпретации знаний
Умение определить уязвимые места в защите информационной системы, выбрать необходимые и экономически обоснованные защитные мероприятия на административном, процедурном и программно-техническом уровнях обеспечения безопасности;	Освоение методик -умение решать практические задачи, выполнять типовые задания: находить уязвимые места в защите информационной системы.
	Умение использовать теоретические знания для выбора методики решения задач, выполнения заданий
	Умение проверять решение и анализировать результаты
	Умение качественно оформлять (презентовать) решение задач и выполнения заданий
Владение навыками применения криптографических пакетов и интерфейсов для построения подсистем информационной безопасности.	Навыки решения стандартных/нестандартных задач: применения криптографических пакетов и интерфейсов для построения подсистем информационной безопасности.
	Объём выполненных заданий
	Качество выполнения трудовых действий
	Самостоятельность планирования выполнения трудовых действий
Использует принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	Знание терминов, определений, понятий: основы построения криптосистем; особенности защити распределенных информационных систем; средства создания и верификации электронных подписей и аутентификации.
	Знание основных закономерностей, соотношений, принципов
	Объем освоенного материала
	Полнота ответов на вопросы
	Четкость изложения и интерпретации знаний
Решает стандартные задачи	Освоение методик -умение решать практические задачи, выполнять типовые задания: реализация криптоалгоритма AES, алгоритма с открытым ключом

профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	RSA, алгоритма обмена ключами Диффи-Хеллмана-Меркла.
	Умение использовать теоретические знания для выбора методики решения задач, выполнения заданий
	Умение проверять решение и анализировать результаты
	Умение качественно оформлять (презентовать) решение задач и выполнения заданий
Подготавливает обзоры, аннотации, составляет рефераты, научные доклады, публикации и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Навыки решения стандартных/нестандартных задач: адаптации и применения существующих систем защиты информации от несанкционированного доступа.
	Объём выполненных заданий
	Качество выполнения трудовых действий
	Самостоятельность планирования выполнения трудовых действий

Оценка преподавателем выставляется интегрально с учётом всех показателей и критериев оценивания.

Оценка сформированности компетенций по показателю Знания.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Знание терминов, определений, понятий	Не знает терминов и определений	Знает термины и определения, но допускает неточности формулировок	Знает термины и определения	Знает термины и определения, может корректно сформулировать их самостоятельно
Знание основных закономерностей, соотношений, принципов	Не знает основные закономерности и соотношения, принципы построения знаний	Знает основные закономерности, соотношения, принципы построения знаний	Знает основные закономерности, соотношения, принципы построения знаний, их интерпретирует и использует	Знает основные закономерности, соотношения, принципы построения знаний, может самостоятельно их получить и использовать
Объем освоенного материала	Не знает значительной части материала дисциплины	Знает только основной материал дисциплины, не усвоил его деталей	Знает материал дисциплины в достаточном объеме	Обладает твердым и полным знанием материала дисциплины, владеет дополнительными знаниями
Полнота ответов на вопросы	Не дает ответы на большинство вопросов	Дает неполные ответы на все вопросы	Дает ответы на вопросы, но не все - полные	Дает полные, развернутые ответы на поставленные вопросы
Четкость изложения и интерпретации знаний	Излагает знания без логической последовательности	Излагает знания с нарушениями в логической последовательности	Излагает знания без нарушений в логической последовательност и	Излагает знания в логической последовательности, самостоятельно их интерпретируя и

				анализируя
	Не иллюстрирует изложение поясняющими схемами, рисунками и примерами	Выполняет поясняющие схемы и рисунки небрежно и с ошибками	Выполняет поясняющие рисунки и схемы корректно и понятно	Выполняет поясняющие рисунки и схемы точно и аккуратно, раскрывая полноту усвоенных знаний
	Неверно излагает и интерпретирует знания	Допускает неточности в изложении и интерпретации знаний	Грамотно и по существу излагает знания	Грамотно и точно излагает знания, делает самостоятельные выводы

Оценка сформированности компетенций по показателю Умения.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Освоение методик - умение решать практические задачи, выполнять типовые задания	Не умеет решать практические задачи, выполнять типовые задания	С дополнительной помощью может решать практические задачи, выполнять типовые задания, допускает ошибки	Допускает неточности при решении практических задач и выполнении типовых заданий	Грамотно использует методики, умеет решать все практические задачи, выполнять все типовые задания
Умение использовать теоретические знания для выбора методики решения задач, выполнения заданий	Не умеет использовать теоретические знания для выбора методики решения задач, выполнения заданий	С дополнительной помощью может выполнить выбор методики решения задач. При выполнении заданий допускает ошибки	Умеет использовать теоретические знания для выбора методики решения задач, допускает неточности при выполнении заданий	Самостоятельно может сделать выбора методики решения задач, выполняет все задания без ошибок
Умение проверять решение и анализировать результаты	Не умеет проверять решение и анализировать результаты	Проверять решение, с дополнительной помощью может анализировать результаты	Проверяет решение в достаточном объеме, при анализе результатов допускает неточности	Обладает твердыми умениями проверки решения и анализа результатов
Умение качественно оформлять (презентовать) решение задач и выполнения заданий	Не умеет качественно оформлять (презентовать) решение задач и выполнения заданий	Выполняет поясняющие схемы и рисунки небрежно и с ошибками	Выполняет оформление решения задач и выполнения заданий корректно и понятно	Качественно и на высоком уровне оформляет решение задач и выполнения заданий

Оценка сформированности компетенций по показателю Иметь навыки.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Навыки решения стандартных/нестандартных задач	Не может выполнять решения стандартных задач	С дополнительной помощью может выполнить решения стандартных/нестандартных задач, допускает ошибки	Может выполнить решение стандартных/нестандартных задач, но допускает неточности	Самостоятельно может выполнить решение стандартных/нестандартных задач
Объём	Не выполняет	Выполняет задания	Выполняет задания	Выполняет весь

выполненных заданий	значительную часть заданий по дисциплине	только по основному материалу дисциплины, не усвоил его деталей	в достаточном объеме	объём заданий. Обладает твердым и полным знанием материала дисциплины, владеет дополнительными знаниями
Качество выполнения трудовых действий	Не выполняет трудовые действия	Имеет навыки выполнения трудовых действий только по основному материалу дисциплины, не усвоил его деталей	Имеет навыки выполнения трудовых действий в достаточном объеме	Обладает твердыми навыками выполнения трудовых действий по всему материалу дисциплины, владеет дополнительными навыками
Самостоятельность планирования выполнения трудовых действий	Не выполняет планирования выполнения трудовых действий	Допускает неточности при планировании выполнения трудовых действий	Самостоятельно и грамотно выполняет планирование выполнения большинства трудовых действий	Самостоятельно и грамотно выполняет планирование выполнения всех трудовых действий

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

6.1. Материально-техническое обеспечение

№	Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1	Аудитория для лекционных занятий	оборудованы специализированной мебелью, мобильным или стационарным мультимедийным проектором, переносным экраном, ноутбуком, или компьютером на базе одно или двухъядерных процессоров с тактовой частотой не менее 2 ГГц, объемом оперативной памяти не менее 2 Гб и жесткого диска до 500 Гб; локальная сеть с пропускной способностью 100 Мбит/с
2	Компьютерные классы для проведения лабораторных занятий	оборудованы специализированной мебелью, компьютерами с установленными программными продуктами на базе одно или двухъядерных процессоров с тактовой частотой не менее 2 ГГц, объемом оперативной памяти не менее 2 Гб и жесткого диска до 500 Гб; локальная сеть с пропускной способностью 100 Мбит/с, принтеры или многофункциональные устройства форматов А4, А3.
3	Помещения для самостоятельной работы обучающихся	оборудованы специализированной мебелью, компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации

6.2. Лицензионное и свободно распространяемое программное обеспечение

№	Перечень лицензионного программного обеспечения.	Реквизиты подтверждающего документа
1	Microsoft Office Professional Plus 2016	Соглашение Microsoft Open Value Subscription V6328633. Соглашение действительно с 02.10.2017 по 31.10.2023
2	Microsoft Windows 10 Корпоративная	Соглашение Microsoft Open Value Subscription V6328633. Соглашение действительно с 02.10.2017 по 31.10.2023). Договор поставки ПО 0326100004117000038-0003147-01 от 06.10.2017
3	Kaspersky Endpoint Security «Стандартный Russian Edition»	Сублицензионный договор № 102 от 24.05.2018. Срок действия лицензии до 19.08.2020 Гражданско-правовой Договор (Контракт) № 27782 «Поставка продления права пользования

		(лицензии) Kaspersky Endpoint Security от 03.06.2020. Срок действия лицензии 19.08.2022г.
4	Google Chrome	Свободно распространяемое ПО согласно условиям лицензионного соглашения
5	Mozilla Firefox	Свободно распространяемое ПО согласно условиям лицензионного соглашения
6	Microsoft Visual Studio 2013	договор №63-14кот 02.07.2014
7	Система компьютерного тестирования знаний VeralTest (сетевая версия VeralSoft без ограничений)	электронное письмо от 06.04.2008

6.3. Перечень учебных изданий и учебно-методических материалов

1. Шаньгин, В. Ф. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / Шаньгин В. Ф. - Москва : ДМК Пресс, 2014. - 702 с. http://www.iprbookshop.ru/63594.html?replacement=1/
2. Скрипник, Д. А. Общие вопросы технической защиты информации [Электронный ресурс] : учебное пособие / Скрипник Д. А. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 264 с. http://www.iprbookshop.ru/52161.html?replacement=1
3. Аверченков В.И., Рытов М.Ю. Организационная защита информации Учебное пособие Брянский государственный технический университет 2012 http://www.iprbookshop.ru/7002.html
4. Смышляев А. Г. Информационная безопасность и защита информации : метод. указания к выполнению лаб. работ / БГТУ им. В. Г. Шухова, каф. информ. технологий ; сост. А. Г. Смышляев. - Белгород : Изд-во БГТУ им. В. Г. Шухова, 2008. - 27 с.
5. Аверченков, В. И. Аудит информационной безопасности [Электронный ресурс] : учебное пособие для вузов / Аверченков В. И. - Брянск : Брянский государственный технический университет, 2012. - 268 с. http://www.iprbookshop.ru/6991.html
6. Гашков, С. Б. Криптографические методы защиты информации : учеб. пособие / С. Б. Гашков, С. Б. Применко, М. А. Черепнев. - Москва : Академия, 2010. - 298 с.
7. Смышляев А. Г. Информационная безопасность : лаб. практикум : учеб. пособие / А. Г. Смышляев ; БГТУ им. В. Г. Шухова. - Белгород : Изд-во БГТУ им. В. Г. Шухова, 2015. - 101 с.
8. Петренко, С. А. Политики безопасности компании при работе в Интернет [Текст] / Петренко С. А. - Саратов : Профобразование, 2017. - 397 с. http://www.iprbookshop.ru/63807
9. Аверченков, В. И. Аудит информационной безопасности [Электронный ресурс] : учебное пособие для вузов / Аверченков В. И. - Брянск : Брянский государственный технический университет, 2012. - 268 с. http://www.iprbookshop.ru/7002
10. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие Учебное пособие М.: Книжный мир 2009 http://biblioclub.ru/index.php?page=book&id=89798
11. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности [Электронный ресурс] : учебное пособие / Авдошин С. М. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2010. - 326 с. http://biblioclub.ru/index.php?page=book&id=233684
12. Спицын, В. Г. Информационная безопасность вычислительной техники [Электронный ресурс] : учебное пособие / Спицын В. Г. - Томск : Эль Контент, Томский государственный университет систем управления и радиоэлектроники, 2011. - 148 с.

http://www.iprbookshop.ru/13936.html
13. Федин, Ф. О. Информационная безопасность [Электронный ресурс] : учебное пособие / Федин Ф. О. - Москва : Московский городской педагогический университет, 2011. - 260 с. http://www.iprbookshop.ru/26486.html
14. Лапонина, О. Р. Основы сетевой безопасности : криптографические алгоритмы и протоколы взаимодействия : учеб. пособие / О. Р. Лапонина. - 2-е изд., испр. . - Москва : Интернет-Университет Информационных Технологий ; Москва : БИНОМ. Лаборатория знаний, 2007. - 531 с.
15. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие / В. В. Платонов. - Москва : Академия, 2006. - 239 с

6.4. Перечень интернет ресурсов, профессиональных баз данных, информационно-справочных систем

1. Портал по информационной безопасности [Электронный ресурс]. Режим доступа: http://infosecurity.report.ru
2. Российский криптографический портал [Электронный ресурс]. Режим доступа: http://infosecurity.report.ru
3. Сервер компании НИП "Информзащита" [Электронный ресурс]. Режим доступа: http://infosecurity.report.ru
4. Информационный бюллетень "Jet Info" [Электронный ресурс]. Режим доступа: http://infosecurity.report.ru
5. Портал по информационной безопасности [Электронный ресурс]. Режим доступа: http://bugtraq.ru