МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета экономики менеджмента и информационных технологий

_____ С.А.Баркалов

«30» августа 2017 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Информационная безопасность и защита информации»

Направление подготовки 09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

Профиль Информационные системы и технологии в стрроительстве

Квалификация выпускника Бакалавр
Нормативный период обучения 4 года
Форма обучения очная
Год начала подготовки 2017

Автор программы _____/Маковий К.А./

Заведующий кафедрой Информационных технологий и автоматизированного проектирования в строительстве _____/Смольянинов А.В./

Руководитель ОПОП _____/Курипта О.В./

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

Целью дисциплины является формирование у обучаемых знаний в области теоретических основ информационной безопасности (ИБ) и навыков практического обеспечения защиты информации в организации

1.2. Задачи освоения дисциплины

Задачи освоения дисциплины - научить правовым основам информационной безопасности на предприятии, организационным и техническим методам и средствам обеспечения информационной безопасности, аудиту информационной безопасности предприятия и организации. Важной задачей освоения дисциплины является способность применять системный подход к обеспечению информационной безопасности телекоммуникационных систем

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Информационная безопасность и защита информации» относится к дисциплинам вариативной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Информационная безопасность и защита информации» направлен на формирование следующих компетенций:

ОПК-4 - пониманием сущности и значения информации в развитии современного общества, соблюдение основных требований к информационной безопасности, в том числе защиты государственной тайны

ПК-1 - способность проводить предпроектное обследование объекта проектирования, системный анализ предметной области, их взаимосвязей

ПК-6 - способность оценивать надежность и качество функционирования объекта проектирования

ДПК-3 - способность обнаруживать угрозы безопасности и устранять нарушения целостности данных

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-4	знать концепцию информационной безопасности Российской Федерации и основные нормативные правовые акты в области информационной безопасности и защиты информации
	уметь выявлять угрозы информационной безопасности
	Владеть навыками структурирования информационных ресурсов в соответствии с их ценностью и уровнем конфиденциальности,

	определения необходимости их защиты от несанкционированного доступа
ПК-1	знать принципы криптографических преобразований
	уметь обосновывать организационно-технические мероприятия по защите информации в ИС
	владеть методами обеспечения безопасного сетевого взаимодействия
ПК-6	знать классификацию и характеристики каналов утечки информации
	уметь анализировать уровень эффективности используемых средств и методов защиты информации
	владеть терминологией в области информационной безопасности и защиты информации
ДПК-3	знать аспекты информационной безопасности
	уметь выявлять угрозы информационной безопасности
	Владеть навыками классификации угроз информационной безопасности

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Информационная безопасность и защита информации» составляет 5 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		8
Аудиторные занятия (всего)	56	56
В том числе:		
Лекции	28	28
Лабораторные работы (ЛР)	28	28
Самостоятельная работа	88	88
Курсовая работа	+	+
Часы на контроль	36	36

Виды промежуточной аттестации - экзамен	+	+
Общая трудоемкость академические часы з.е.	180 5	180 5

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Введение. Основные понятия в области информационной безопасности. Наиболее распространенные угрозы ИБ.	Понятие информационной безопасности (ИБ). Защита информации, задачи защиты информации. Угрозы ИБ. Основные аспекты ИБ: доступность, целостность, конфиденциальность. Угроза, атака, злоумышленник - источник угрозы. Понятие окна опасности. Необходимость своевременного обновления ПО.. Критерии классификации угроз: по аспекту ИБ, по компонентам ИС, по способу осуществления, по расположению источника угроз. Примеры угроз доступности, угроз конфиденциальности, угроз целостности. Уровни обеспечения ИБ. Понятие национальной безопасности: виды безопасности: государственная, экономическая, общественная, военная, экологическая, информационная; роль и место системы обеспечения ИБ в системе национальной безопасности РФ.	6	6	14	26
2	Законодательный уровень ИБ.	Законодательные меры обеспечения ИБ. Меры ограничительной и меры созидательной направленности. Правовые акты общего назначения, затрагивающие вопросы ИБ. Конституция РФ — статьи 24, 41, 42, 23, Гражданский кодекс РФ, Уголовный кодекс РФ, Закон РФ N 5485-1 «О государственной тайне», N 149-ФЗ «Об информации, информационных технологиях и о защите информации», N 63-ФЗ «Об электронной подписи», N 152-ФЗ «О персональных данных», N 098-ФЗ «О коммерческой тайне». Приказ ФАПСИ от 13 июня 2001 г. N 152.	6	6	14	26

3	Программно-технический уровень обеспечения ИБ. Введение в криптографию. Инфраструктура открытых ключей (Public Key Infrastructure PKI).	Основные понятия криптографии: шифрование, симметричное шифрование и ассиметричное шифрование**.** Понятие ключа шифрования, открытого (plaintext) и зашифрованного (ciphertext) сообщения. Криптографический алгоритм, структура алгоритма симметричного шифрования. Операции, используемые в современных алгоритмах симметричного шифрования: S-box, перемещение, сложение по модулю 2, циклический сдвиг. Сеть Фейштеля, структура сети, понятие раунда. Структура алгоритма DES, преобразования ключа, преобразование данных. Проблемы симметричного шифрования. История создания алгоритмов асимметричного шифрования. Алгоритм Диффи-Хеллмана, алгоритм RSA, алгоритм DSS, сравнительная характеристика и области применения. Понятие хэш-функции. Требования к хэш-функции, используемой для аутентификации сообщений. Слабая и сильная хэш-функция. Пример использованияхэш-функции для хэширования паролей в ОС. Современные хэш-функции: MD5, SHA-1, SHA-2, SHA-3. Российские стандарты в области криптографии: алгоритм симметричного шифрования ГОСТ 28147-89, хэш-функция ГОСТ 34.11-2012. Цифровая подпись, необходимые свойства. Использование алгоритмов асимметричного шифрования для создания цифровой подписи документа. Стандарты DSS и ГОСТ 34.10-2012. Детерминированные и рандомизированные цифровые подписи. Понятие инфраструктуры открытых ключей (Public Key Infrastructure PKI). Технические средства защиты информации. Защита информации от утечки по техническим каналам. Сертифицированные средства защиты информации.	4	4	14	22
4	Административный и процедурный уровень обеспечения ИБ.	Понятие политики безопасности как основного документа организации в области ИБ. Уровни политики безопасности и содержание каждого уровня. Тестирование процедур и механизмов безопасности. Аварийный план. Регламент реагирования на	4	4	14	22

		нарушение информационной безопасности. Аудит безопасности. . Классификация ИС по требованиям по требованиям защиты информации. Обработка персональных данных (ПДн). Классификация систем обработки ПДн. Базовая модель угроз безопасности ПД при их обработке в ИСПДн ФСТЭК России. Синхронизация программы безопасности с жизненным циклом ИС.				
5	Обеспечение безопасности обработки ин- формации в распределенных вычислительных системах.	Компьютерные вирусы, классификация. Средства защиты и регламент организации антивирусной защиты. Понятие межсетевого экрана, основное назначение и функции. Типы межсетевых экранов. Методы соединения сети организации с сетью Интернет: брандмауэр, прокси-сервер, SOCKS4, SOCKS5, NAT, PAT. Демилитаризованная зона DMZ.	4	4	16	24
6	Методы обеспечения безопасного сетевого взаимодействия. Виртуальные частные сети.	Виртуальные частные сети, тунеллирующие протоколы. Типы VPN соединения. Основные технологии VPN: PPTP, L2TP. Аутентификация и шифрование в протоколах PPTP и L2TP.	4	4	16	24
		Итого	**28**	**28**	**88**	**144**

5.2 Перечень лабораторных работ

1. Изучение разрешений NTFS и разрешений на общий ресурс в операционной системе Windows 7.
2. Изучение аудита в операционной системе Windows 7.
3. Установка и настройка центра сертификации на базе служб сертификации Active Directory Windows Server 2008.
4. Настройка шифрования и подписи документов в Windows 7.
5. Настройка VPN тоннеля.

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсовой работы в 8 семестре для очной формы обучения.

Примерная тематика курсовой работы: «Разработка и внедрение решения по безопасному информационному обмену между двумя и более абонентами, территориально удаленными друг от друга»

Задачи, решаемые при выполнении курсовой работы:

- Анализ предметной области и возможных способов решения задачи проекта, формулировка задачи проекта
- Выбор средств реализации задачи проекта и его обоснование
- Реализация проекта с учетом ограничения ресурсов и требований информационной безопасности

Курсовая работа включат в себя графическую часть и расчетно-пояснительную записку.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

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

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-4	знать концепцию информационной безопасности Российской Федерации и основные нормативные правовые акты в области информационной безопасности и защиты информации	Активное участие в устных опросах на занятиях, правильно отвечает на теоретические вопросы при защите курсовой работы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь выявлять угрозы информационной безопасности	Выполнение лабораторных работ, оформление курсовой работы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть навыками структурирования информационных ресурсов в соответствии с их ценностью и уровнем конфиденциальности, определения необходимости их защиты от несанкционированного доступа	Выполнение лабораторных работ, курсовой работы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-1	знать принципы криптографических преобразований	Активное участие в устных опросах на занятиях, правильно отвечает на теоретические вопросы при защите курсовой работы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь обосновывать организационно-технические мероприятия по защите информации в ИС	Выполнение лабораторных работ, оформление курсовой работы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть методами обеспечения безопасного сетевого взаимодействия	Выполнение лабораторных работ, курсовой работы	Выполнение работ в срок, предусмотренный в рабочих	Невыполнение работ в срок, предусмотренный в рабочих

			программах	программах
ПК-6	Знать классификацию и характеристики каналов утечки информации	Активное участие в устных опросах на занятиях, правильно отвечает на теоретические вопросы при защите курсовой работы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь анализировать уровень эффективности используемых средств и методов защиты информации	Выполнение лабораторных работ, оформление курсовой работы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть терминологией в области информационной безопасности и защиты информации	Выполнение лабораторных работ, курсовой работы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ДПК-3	Знать аспекты информационной безопасности	Активное участие в устных опросах на занятиях, правильно отвечает на теоретические вопросы при защите курсовой работы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь выявлять угрозы информационной безопасности	Выполнение лабораторных работ, оформление курсовой работы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть навыками классификации угроз информационной безопасности	Выполнение лабораторных работ, курсовой работы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 8 семестре для очной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компе-тенция	**Результаты обучения, характеризующие сформированность компетенции**	**Критерии оценивания**	**Отлично**	**Хорошо**	**Удовл.**	**Неудовл.**
ОПК-4	знать концепцию информационной безопасности Российской Федерации и основные нормативные правовые акты в области информационной безопасности и защиты информации	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь выявлять угрозы информационной	Решение стандартных	Задачи решены в	Продемонстр ирован	Продемонстр ирован	Задачи не решены

	безопасности	практических задач	полном объеме и получены верные ответы	верный ход решения всех, но не получен верный ответ во всех задачах	верный ход решения в большинстве задач	
	Владеть навыками структурирования информационных ресурсов в соответствии с их ценностью и уровнем конфиденциальности, определения необходимости их защиты от несанкционированного доступа	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
ПК-1	знать принципы криптографических преобразований	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь обосновывать организационно-технические мероприятия по защите информации в ИС	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
	владеть методами обеспечения безопасного сетевого взаимодействия	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
ПК-6	знать классификацию и характеристики каналов утечки информации	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь анализировать уровень эффективности используемых средств и методов защиты информации	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
	владеть терминологией в области информационной безопасности и защиты информации	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены

ДПК-3	знать аспекты информационной безопасности	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь выявлять угрозы информационной безопасности	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
	Владеть навыками классификации угроз информационной безопасности	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. Под Информационной безопасностью (ИБ) понимают:
   - Защита пользователя от вредоносной информации
   - **Защищенность информации от непреднамеренных действий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений**
   - **Защищенность поддерживаемой инфраструктуры от непреднамеренных действий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений**
   - Комплекс мер по защите информации
2. К основным задачам обеспечения ИБ относятся:
   - **Обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры**
   - Защита информации и субъектов информационных отношений
   - Защита от несанкционированного доступа к конфиденциальным данным;
   - Обеспечение соблюдения государственной тайны, и защиты от несанкционированного доступа.
3. Что из перечисленного не относится к мерам по обеспечению ИБ?
   - Законодательные меры
   - **Экономические меры обеспечения ИБ**.
   - Административные и процедурные меры по обеспечению ИБ;
   - Программно-технические меры по обеспечению ИБ.
4. Окном опасности ПО называют

- Время наиболее вероятного проникновения в информационную систему;
- **Промежуток времени от момента обнаружения слабого места до момента установки соответствующей «заплатки»;**
- Промежуток времени с 03:00 до 06:00, когда совершается большинство правонарушений
- Промежуток времени до обнаружения уязвимости ИС.

5. Что понимается под угрозой безопасности информации в компьютерной системе:
   - потенциально возможная уязвимость информации в компьютерной системе.
   - потенциально возможное событие, которое может привести к уничто- жению, утрате целостности, конфиденциальности или доступности ин- формации.
   - подготовка взлома компьютерной системы.
6. Какие из перечня угроз относятся к случайным угрозам компьютерной информации:
   - несанкционированный доступ к информации, вредительские программы, ошибки при разработке компьютерной системы;
   - электромагнитные излучения и наводки, несанкционированная модифика- ция структуры компьютерной системы;
   - стихийные бедствия и аварии, сбои и отказы технических средств, ошибки пользователей и обслуживающего персонала;
7. Для защиты от случайных угроз компьютерной информации используют:
   - обучение пользователей правилам работы с информационной системой, разрешительную систему доступа в помещение;
   - межсетевые экраны, идентификацию и аутентификацию пользователей;
   - дублирование информации, создание отказоустойчивых КС, блокировку ошибочных операций.
8. Построение модели злоумышленника при создании системы защиты информации необходимо для:
   - **оптимизации системы защиты информации.**
   - составления фоторобота злоумышленника.
   - составления базы данных потенциальных взломщиков
9. Какие из перечня угроз относятся к преднамеренным угрозам компьютерной информации:
   - **шпионаж и диверсии, несанкционированный доступ к информации, вредоносные программы;**
   - ошибки при разработке компьютерной системы, ошибки в программном обеспечении, электромагнитные излучения и наводки;
   - стихийные бедствия и аварии, сбои и отказы технических средств, ошибки пользователей и обслуживающего персонала;

10. Какие средства защиты фиксируют факт проникновения злоумышленника в компьютерную систему?
    - средства охранно-пожарной сигнализации;
    - средства биометрической идентификации;
    - **пломбы, наклейки, замки на аппаратуре компьютерной системы.**

11. Какие компьютерные системы называются защищенными:
    - **в которых обеспечивается безопасность информации.**
    - в которых установлены программно-аппаратные средства защиты инфор мации.
    - которые размещены в защищенном помещении.

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Идентификация это:
    - процесс предъявления пользователем идентификатора;
    - процесс подтверждения подлинности;
    - **сравнение предъявляемых идентификаторов с перечнем присвоенных идентификаторов.**
2. Аутентификация это:
    - процесс предъявления пользователем идентификатора;
    - **процесс подтверждения подлинности**;
    - регистрация всех обращений к защищаемой информации;
3. К средствам опознавания пользователя компьютерной системой относятся:
    - паспорт, студенческий билет.
    - фотография, подпись.
    - **пароли, пластиковые карты**
4. Несанкционированный доступ к информации в компьютерной системе это:
    - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств вычислительной техники;
    - доступ к информации, нарушающий правила разграничения доступа с использованием технических средств разведки;
    - **доступ к информации компьютерной системы без санкции администратора безопасности.**
5. Что относится к основным механизмам защиты компьютерной системы от несанкционированного доступа:
    - **физическая защита компонент компьютерной системы и носителей информации, идентификация и аутентификация, разграничение доступа**;
    - дублирование информации, создание отказоустойчивых

компьютерных систем, блокировка ошибочных операций;
- сегментация сетей с помощью коммутаторов и межсетевых экранов, шифрование информации.

6. Какие основные способы разграничения доступа применяются в компьютерных системах:
   - **дискреционный и мандатный.**
   - по специальным спискам и многоуровневый.
   - по группам пользователей и специальным разовым разрешениям**.**
7. Какой приоритет учитывается при планировании разрешений доступа для файлов и папок?
   - Приоритет разрешения над запрещением**.**
   - **Приоритет запрещения над разрешением.**
   - Приоритет разрешений для папок над разрешениями для файлов.
   - Приоритет разрешений для файлов над разрешениями для папок
8. Что такое аудит безопасности?
   - Это инструмент политики безопасности, позволяющий контролировать процесс загрузки системных драйверов.
   - **Это инструмент политики безопасности, позволяющий отслеживать действия пользователей и системные события и регистрировать их в журнале**.
   - Это инструмент политики безопасности, позволяющий наблюдать динамические изменения технического состояния аппаратных компонентов компьютера (температура материнской платы, скорость враще- ния вентилятора на процессоре и т.д.).

9. Кто должен анализировать журнал аудита безопасности компьютерной системы:
   - Администратор;
   - Пользователь;
   - **Аудитор;**
   - директор.
10. Средства шифрования с асимметричными ключевыми системами применяют:
    - для создания резервных копий конфиденциальной информации.
    - для шифрования конфиденциальной информации на компьютере.
    - **для обмена конфиденциальными сообщениями в компьютерных сетях**
    - **для обмена ключом симметричного шифрования**.
11. Автоматическое шифрование незаметное для пользователя называют:
    - прозрачное.
    - Зеркальное
    - Тайное
    - призрачное.
12. Для создания цифровой подписи следует использовать:

- Свой открытый ключ
- **Свой закрытый ключ**
- Открытый ключ получателя
- Закрытый ключ получателя

13. Для проверки цифровой подписи следует использовать
    - Свой открытый ключ
    - Свой закрытый ключ
    - **Открытый ключ отправителя**
    - Закрытый ключ отправителя
14. Выберите правильное высказывание:
    - **Алгоритм ГОСТ 28147 -89 использует постоянные S-boxes**
    - Алгоритм ГОСТ 28147 -89 использует переменные S-boxes, зависящие от ключа
    - Алгоритм ГОСТ 28147 -89 не использует S-boxes
15. Для контроля целостности программной структуры в процессе эксплуатации ис- пользуется:
    - **контрольное суммирование, хэш-функция;**
    - сравнение параметров рабочих программных файлов с дистрибутивами;
    - проверка списка файлов программного обеспечения.
16. Для обеспечения эффективной защиты информации в базах данных необходимо наличие:
    - средств шифрования файлов и папок;
    - **встроенных в систему управления базой данных функций защиты;**
    - встроенных в операционную систему функций защиты**.**

7.2.3 Примерный перечень заданий для решения прикладных задач

1. Наличие встроенных средств защиты информации в операционной системе:
    - мешает дополнительным средствам защиты компьютерной системы.
    - усложняет управление комплексной системой защиты информации.
    - **усиливает защищенность компьютерной системы.**
2. Для создания доверенного соединения сетевого клиента с сервером:
    - сервер должен распознать (аутентифицировать) клиента.
    - клиент должен распознать (аутентифицировать) сервер.
    - **клиент и сервер должны распознать друг друга.**
3. Электронная цифровая подпись - это:
    - **реквизит электронного документа в виде цифровой последовательности, предназначенный для защиты его от изменения. Позволяет идентифицировать владельца**.
    - реквизит электронного документа в виде изображения подписи владельца, предназначенный для защиты документа от изменения.

- реквизит электронного документа в виде изображения подписи владельца, предназначенный для идентификации владельца.

4. Межсетевые экраны предназначены для:
   - Обнаружения сетевых атак или подозрительных намерений.
   - **разграничения доступа между двумя сетями с различными требова- ниями по обеспечению безопасности.**
   - контроля почтового трафика и Web-трафика**.**
5. Какой принцип управления межсетевым экраном предпочтительнее в компьютерной системе, обрабатывающей конфиденциальную информацию:
   - разрешено все, что не запрещено.
   - **запрещено все, что не разрешено**.
   - выборочной фильтрации трафика.
6. Одной из основных функций систем виртуальной частной сети (VPN) является:
   - сокрытия факта передачи информации по цифровым сетям связи.
   - **сокрытия информации заголовка сетевого пакета**.
   - шифрования данных в сетевом пакете.
7. Политика безопасности организации это:
   - перечень параметров настройки системы безопасности.
   - инструкции пользователям компьютерной системы по применению средств защиты информации.
   - **пакет документов регламентирующих деятельность по защите информации.**
8. Оценка и управление рисками информационной безопасности необходимы для:
   - оценки ущерба от информационной атаки злоумышленника.
   - **построения оптимальной системы защиты информации**.
   - построения системы разграничения доступа к информации.
9. Системы анализа уязвимостей позволяют:
   - выявить злоумышленника работающего в компьютерной сети.
   - выявить уязвимости проектируемой системы защиты информации.
   - **выявить уязвимости действующей системы защиты информации.**
10. Для оперативного восстановления работоспособности компьютерной системы необходимо наличие
    - RAID системы.
    - дистрибутива операционной системы и программ.
    - **загрузочного диска и образа системы.**
11. Компьютерные вирусы - это
    - **программы, характерной особенностью которых является способность к размножению (саморепликации)**;
    - программы, которые внедряются в компьютер с целью получения информации;

- программы, которые возникают и распространяются независимо от человека.

12. Для организации службы защиты информации на предприятии
    - достаточно руководствоваться только федеральными законами.
    - достаточно руководствоваться федеральными законами и ведомственными нормативными актами.
    - **необходимо дополнительно разработать собственные руководящие документы**.
13. Объектами защиты информации в компьютерной системе являются:
    - накопители информации.
    - каналы передачи данных
    - пользователь.
    - **все перечисленное**.

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный перечень заданий для подготовки к экзамену

1. Понятие информационной безопасности, основные составляющие и задачи обеспечения ИБ. Угроза, атака, злоумышленник.
2. Типы и критерии классификации угроз ИБ. Основные угрозы по аспектам ИБ
3. Окно опасности, обновление ПО, технологии автоматизации обновления ПО.
4. Государственное регулирование в области информационной безопасности.
5. Меры обеспечения ИБ. Законодательные меры обеспечения ИБ. Основные законодательные акты регулирования в области ИБ
6. Ответственность за нарушение правовых норм защиты информации.
7. Основные правовые акты, регулирующие деятельность в области обеспечения ИБ.
8. Доктрина ИБ России, регламентирующие документы ФСТЭК России.
9. Основные понятия криптографии: тип шифрования, ключ шифрования, открытый и зашифрованный текст.
10. Требования к криптографическим алгоритмам.
11. Программно-технические меры обеспечения ИБ. Криптография. Симметричное шифрование. Типы алгоритмов симметричного шифрования Современные алгоритмы ассиметричного шифрования, область применения каждого из алгоритмов.
12. Программно-технические меры обеспечения ИБ. Структура алгоритма симметричного шифрования. Сеть Фейштеля. Алгоритм DES.
13. Программно-технические меры обеспечения ИБ. Современные алгоритмы симметричного шифрования.
14. Программно-технические меры обеспечения ИБ. Проблемы симметричного шифрования. Требования к алгоритмам асимметричного шифрования.

15. Программно-технические меры обеспечения ИБ. Алгоритм Диффи-Хеллмана, алгоритм RSA.
16. Программно-технические меры обеспечения ИБ. Применение хэш-функции для идентификации сообщений. Отличие слабой и сильной хэш-функции.
17. Программно-технические меры обеспечения ИБ. Электронно-цифровая подпись. Стандарты цифровой подписи.
18. Российские стандарты в области криптографии: алгоритм симметричного шифрования, хэш-функции, цифровой подписи.
19. Инфраструктура открытых ключей (PKI). Понятие, компоненты и структура PKI.
20. Инфраструктура открытых ключей (PKI). Центр сертификации (CA) реализации Microsoft. Варианты иерархии, особенности реализации.
21. Понятие сертификата. Назначение и основные функции.
22. Инфраструктура открытых ключей (PKI). Политика сертификатов и регламент сертификационной практики.
23. Инфраструктура открытых ключей (PKI). Сертификаты, хранилища сертификатов, форматы экспорта сертификатов,
24. Инфраструктура открытых ключей (PKI). Регламент работы с отозванными сертификатами.
25. Методы и средства идентификации и аутентификации пользователей в ОС, СУБД, прикладных программах.
26. Обеспечение безопасности операционной системы: основные методы и технологии.
27. Назначение прав пользователей в ОС: комбинация прав NTFS и разрешений общего доступа.
28. Типы разграничения доступа к ресурсам: мандатное, избирательное и ролевое управление доступом.
29. Аудит операционной системы. Настройка аудита ОС, методология анализа безопасности журнала ОС Windows 7.
30. Настройка шифрования и подписи с ОС Windows 7.
31. Использование сертификатов для шифрования и подписи документов в ОС Windows 7
32. Административные меры обеспечения ИБ. Политика ИБ. Уровни политики ИБ.
33. Административные меры обеспечения ИБ. Синхронизация программы безопасности с жизненным циклом систем.
34. Административные меры обеспечения ИБ. Управление рисками. Этапы процесса управления рисками.
35. Административные меры обеспечения ИБ. Управление рисками. Методологии оценки рисков.
36. Виды компьютерных вирусов. Технологии защиты организации от угрозы заражения компьютерными вирусами.
37. Методы обнаружения известных и неизвестных вирусов.
38. Методы удаления последствий заражения вирусами.

39. Профилактика заражения вирусами КС. Действия пользователя при обнаружении заражения КС вирусами.
40. Применение межсетевых экранов для защиты информации при межсетевом взаимодействии.
41. Методы организации доступа организации к сети Интернет: NAT, PAT, прокси-сервер, SOCKS.
42. Понятие демилитаризованной зоны DMZ. Типовая схема использования DMZ.
43. Виртуальные частные сети (VPN). Основные типы соединений в VPN.
44. Виртуальные частные сети (VPN). Технологии PPTP и L2TP. Шифрование трафика в VPN.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Экзамен проводится по билетам, каждый из которых содержит 2 теоретических вопроса и задачу. Каждый правильный ответ на вопрос в тесте оценивается 5 баллом, задача оценивается в 10 баллов (10 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.)

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Введение. Основные понятия в области информационной безопасности. Наиболее распространенные угрозы ИБ.	ОПК-4, ПК-1, ПК- 6, ДПК-3	Тест, защита лабораторных работ, раскрыта тема в курсовой работе
2	Законодательный уровень ИБ.	ОПК-4, ПК-1, ПК- 6, ДПК-3	Тест, защита лабораторных работ, раскрыта тема в курсовой работе
3	Программно-технический уровень обеспечения ИБ. Введение в криптографию. Инфраструктура открытых ключей (Public Key Infrastructure PKI).	ОПК-4, ПК-1, ПК- 6, ДПК-3	Тест, защита лабораторных работ, раскрыта тема в курсовой работе
4	Административный и процедурный уровень обеспечения ИБ.	ОПК-4, ПК-1, ПК- 6, ДПК-3	Тест, защита лабораторных работ, раскрыта тема в курсовой работе

5	Обеспечение безопасности обработки информации в распределенных вычислительных системах.	ОПК-4, ПК-1, ПК- 6, ДПК-3	Тест, защита лабораторных работ, раскрыта тема в курсовой работе
6	Методы обеспечения безопасного сетевого взаимодействия. Виртуальные частные сети.	ОПК-4, ПК-1, ПК- 6, ДПК-3	Тест, защита лабораторных работ, раскрыта тема в курсовой работе

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Защита курсовой работы, курсового проекта или отчета по всем видам практик осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

1. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональ-ная Академия безопасности и выживания (МАБИВ), 2014.— 256 c.— Режим доступа: http://www.iprbookshop.ru/33430.— ЭБС «IPRbooks», по паролю

2. Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 c. — 978-5-94774-821-5. — Режим доступа: http://www.iprbookshop.ru/52209.html

3. Авдошин С.М. Технологии и продукты Microsoft в обеспечении

информацион-ной безопасности [Электронный ресурс] / С.М. Авдошин, А.А. Савельева, В.А. Сердюк. — Электрон. текстовые данные. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образова-ние, 2017. — 412 c. — 978-5-4487-0147-4. — Режим доступа: http://www.iprbookshop.ru/72341.html

4. Басалова Г.В. Основы криптографии [Электронный ресурс] / Г.В. Басалова. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 282 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/52158.html

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

- операционная система Windows 7, Windows 2008 Server, Linux Mint 19.1;
- интернет браузеры: Yandex Browser, Google Chrome и другие;
- Oracle Virtual Box

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

1. Технические средства:

a. Компьютерный класс с выходом в Интернет.

b. На каждом рабочем месте – ПО Oracle Virtual Box.

c. Проектор.

2. Программное обеспечение:

a. Интернет браузеры: Yandex-Browser, Google Chrome и другие

b. Программа Microsoft Word – текстовый редактор.

c. Программа Adobe Acrobat Reader – средство чтения электрон-ных материалов в формате PDF.

d. Программа MS EXEL –электронные таблицы

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Информационная безопасность и защита информации» читаются лекции, проводятся лабораторные работы, выполняется курсовая работа.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Методика выполнения курсовой работы изложена в учебно-методическом пособии. Выполнять этапы курсовой работы должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсовой работы, защитой курсовой работы.

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

1. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональ-ная Академия безопасности и выживания (МАБИВ), 2014.— 256 c.— Режим доступа: http://www.iprbookshop.ru/33430.— ЭБС «IPRbooks», по паролю

2. Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 c. — 978-5-94774-821-5. — Режим доступа: http://www.iprbookshop.ru/52209.html

3. Авдошин С.М. Технологии и продукты Microsoft в обеспечении информацион-ной безопасности [Электронный ресурс] / С.М. Авдошин, А.А. Савельева, В.А. Сердюк. — Электрон. текстовые данные. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образова-ние, 2017. — 412 c. — 978-5-4487-0147-4. — Режим доступа: http://www.iprbookshop.ru/72341.html

4. Басалова Г.В. Основы криптографии [Электронный ресурс] / Г.В. Басалова. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 282 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/52158.html

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

- операционная система Windows 7, Windows 2008 Server, Linux Mint 19.1;
- интернет браузеры: Yandex Browser, Google Chrome и другие;
- Oracle Virtual Box

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск

	ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.