

УТВЕРЖДАЮ:

Проректор по учебной работе

_____ / О.В. Юсупова

" ____ " _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.01.ДВ.03.02 «Защищенные информационные технологии»

Код и направление подготовки (специальность)	10.03.01 Информационная безопасность
Направленность (профиль)	Комплексная защита объектов информатизации (в промышленности)
Квалификация	Бакалавр
Форма обучения	Очная
Год начала подготовки	2020
Институт / факультет	Институт автоматизации и информационных технологий
Выпускающая кафедра	кафедра "Электронные системы и информационная безопасность"
Кафедра-разработчик	кафедра "Электронные системы и информационная безопасность"
Объем дисциплины, ч. / з.е.	144 / 4
Форма контроля (промежуточная аттестация)	Экзамен

Б1.В.01.ДВ.03.02 «Защищенные информационные технологии»

Рабочая программа дисциплины разработана в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) **10.03.01 Информационная безопасность**, утвержденного приказом Министерства образования и науки РФ от № 1515 от 01.12.2016 и соответствующего учебного плана.

Разработчик РПД:

Доцент, кандидат
технических наук

(должность, степень, ученое звание)

Н.Е Карпова

(ФИО)

Заведующий кафедрой

(ФИО, степень, ученое звание)

СОГЛАСОВАНО:

Председатель методического совета
факультета / института (или учебно-
методической комиссии)

А.Н Дилигенская, доктор
технических наук, доцент

(ФИО, степень, ученое звание)

Руководитель образовательной
программы

Н.Е. Карпова, кандидат
технических наук

(ФИО, степень, ученое звание)

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы	4
2. Место дисциплины (модуля) в структуре образовательной программы	4
3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся	5
4. Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий	5
4.1 Содержание лекционных занятий	6
4.2 Содержание лабораторных занятий	10
4.3 Содержание практических занятий	14
4.4. Содержание самостоятельной работы	14
5. Перечень учебной литературы и учебно-методического обеспечения по дисциплине (модулю)	15
6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения	15
7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем	16
8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)	16
9. Методические материалы	18
10. Фонд оценочных средств по дисциплине (модулю)	19

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Код и наименование компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Общепрофессиональные компетенции	
ОПК-4 способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Владеть навыками проектирования архитектуры системы защиты информации, для обеспечения информационной безопасности объекта, В(ПК-1) -1
	Знать как провести предварительный технико-экономический анализ и обоснование проектных решений по обеспечению информационной безопасности, З(ОПК-4) -1;
	Уметь понимать сущность и значение информации в развитии современного общества, У(ОПК-4) -1;
Профессиональные компетенции	
ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты	Владеть - навыками администрирования подсистем информационной безопасности объекта защиты; - навыками проектирования архитектуры системы защиты информации, для обеспечения информационной безопасности объекта, В(ПК-3) -1
	Знать основы администрирования подсистемы информационной безопасности, З(ПК-3) -1;
	Уметь быстро разобраться в протоколах администрирования подсистемы информационной безопасности объекта защиты, У(ПК-3) -1;

2. Место дисциплины (модуля) в структуре образовательной программы

Место дисциплины (модуля) в структуре образовательной программы: **вариативная часть**

Код компетенции	Предшествующие дисциплины	Параллельно осваиваемые дисциплины	Последующие дисциплины
ОПК-4	Документоведение; Информатика и информационные технологии; Теория информации; Технологии и методы программирования; Учебная практика: ознакомительная практика; Учебная практика: практика по получению первичных профессиональных умений и навыков; Учебная практика: проектная практика; Языки и методы программирования		Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы

ПК-3	Программно-аппаратные средства защиты информации	Защита информационных процессов в компьютерных системах; Производственная практика: эксплуатационная практика	Безопасность вычислительных сетей; Безопасность телекоммуникационных систем; Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы
------	--	---	---

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Вид учебной работы	Всего часов / часов в электронной форме	6 семестр часов / часов в электронной форме
Аудиторная контактная работа (всего), в том числе:	80	80
Лабораторные работы	48	48
Лекции	32	32
Внеаудиторная контактная работа, КСР	4	4
Самостоятельная работа (всего), в том числе:	33	33
подготовка к зачету	13	13
подготовка к лабораторным работам	20	20
Контроль	27	27
Итого: час	144	144
Итого: з.е.	4	4

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

№ раздела	Наименование раздела дисциплины	Виды учебной нагрузки и их трудоемкость, часы				
		ЛЗ	ЛР	ПЗ	СРС	Всего часов
1	Принцип защиты и обеспечения информационной безопасности современных информационных технологий	4	8	0	4	16
2	Принципы шифрования информации	12	16	0	12	40
3	Защита компьютерных систем, реализующих информационные технологии	4	8	0	8	20
4	Защита сетевых информационных технологий	6	8	0	3	17

5	Управление безопасностью информации в автоматизированных системах	6	8	0	6	20	
		КСР	0	0	0	4	
		Контроль	0	0	0	27	
		Итого	32	48	0	33	144

4.1 Содержание лекционных занятий

№ занятия	Наименование раздела	Тема лекции	Содержание лекции (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов / часов в электронной форме
6 семестр				
1	Принцип защиты и обеспечения информационной безопасности современных информационных технологий	Тема 1. Принцип защиты и обеспечения информационной безопасности современных информационных технологий.	1.1 Общая характеристика информационных процессов и технологий и их безопасности. Введение. Понятие информации и информационных процессов, информационных ресурсов. Необходимость защиты информационных ресурсов. Общая характеристика процессов сбора, передачи, накопления и хранения информации. Информационные системы и современные информационные технологии. 1.2 Угрозы современным информационным технологиям. Источники угроз информационным технологиям. Каналы утечки информации. Задачи защиты информационных технологий. Основные принципы защиты информации. Категории и уровни информационной безопасности. 1.3 Компьютерные преступления. Законодательная база по информационным технологиям. Современная классификация компьютерных преступлений. Минимальный список нарушений в области компьютерных преступлений. Законодательная база по информационным технологиям. Ответственность за компьютерные преступления.	2
2	Принцип защиты и обеспечения информационной безопасности современных информационных технологий	Тема 1. Принцип защиты и обеспечения информационной безопасности современных информационных технологий.	1.4 Принципы защиты информации и информационных технологий. Оранжевая книга и общие принципы защиты информации. Политика безопасности и ее функции. 1.5 Теоретические основы защиты информации. Типы и модели политики безопасности. Современные исследования в области защиты информации. 1.6 Модели защиты информации. Управление доступом. Сравнительная характеристика матричных и потоковых моделей защиты информации.	2

3	Принципы шифрования информации	Тема 2. Принципы шифрования информации.	2.1 Принципы криптографической защиты информации. Структуры криптографического преобразования информации. Требования к шифрам, используемым для криптографической защиты информации. Шифры традиционных симметричных криптосистем. 2.2 Криптоаналитические атаки и их классификация. Классификация криптоаналитических атак. Стойкость криптоалгоритма. Причины успешных атак на криптоалгоритмы и методы борьбы с ними.	2
4	Принципы шифрования информации	Тема 2. Принципы шифрования информации	2.3 Простые шифры и системы Цезаря. Шифры перестановки. Шифры простой замены. Аффинная система Цезаря. Система Цезаря с ключевым словом. 2.4 Биграмные шифры и шифры сложной замены. Шифрующие таблицы Трисемуса. Биграмный шифр Плейфейра. Криптосистема Хилла. 2.5 Многоалфавитные шифры. Система шифрования Вижинера. Двойной квадрат Уитстона.	2
5	Принципы шифрования информации	Тема 2. Принципы шифрования информации	2.6 Одноразовые системы шифрования. Одноразовый шифрблокнот. Шифрование методом Вернама. Шифрование гаммированием. Методы генерации псевдослучайных последовательностей. 2.7 Управление ключами в криптосистемах. Асимметричная методология шифрования. Электронно - цифровая подпись. Усиленная аутентификация. 2.8 Современные криптосистемы. Классификация современных алгоритмов шифрования. Блочные и поточные алгоритмы. Симметричная и асимметричная методологии. Методы реализации криптосистем.	2
6	Принципы шифрования информации	Тема 2. Принципы шифрования информации	2.9 Симметричные криптосистемы. Криптосистема DES. Принцип итерирования и конструкция Фейстеля. Основные режимы блочного шифрования. Стандарт шифрования данных DES. Цикл преобразования в криптосистеме DES. 2.10 Современные блочные симметричные криптосистемы. Комбинирование блочных алгоритмов. Алгоритм шифрования IDEA. Отечественный стандарт шифрования данных ГОСТ 28147-89. Сравнительная оценка симметричных криптосистем.	2

7	Принципы шифрования информации	Тема 2. Принципы шифрования информации	2.11 Асимметричные криптосистемы. Односторонние функции. Проблемы факторизации и дискретного логарифмирования больших чисел. 2.12 Стандарт асимметричного шифрования RSA. Алгоритмические преобразования в системе RSA. Процессы шифрования и расшифровывания. Криптостойкость и быстродействие системы RSA. 2.13 Распространенные асимметричные и комбинированные схемы шифрования. Схема шифрования Полига-Хелмана. Схема шифрования Эль Гамала.	2
8	Принципы шифрования информации	Тема 2. Принципы шифрования информации	2.14 Проблема аутентификации данных и электронно-цифровая подпись. Однонаправленные хеш-функции. Схемы формирования ЭЦП (алгоритмы RSA, EGSA, DSA). Отечественный стандарт ЭЦП. 2.15 Идентификация и проверка подлинности. Идентификация и аутентификация пользователя. Взаимная проверка подлинности. Протоколы идентификации с нулевой передачей знаний. 2.16 Управление криптографическими ключами. Генерация и хранение ключей. Распределение ключей. 2.17 Новые направления в шифровании информации. "Шарады" с временным замком. Квантовая криптография. Компьютерная стеганография. Электронные водяные знаки.	2
9	Защита компьютерных систем, реализующих информационные технологии	Тема 3 Защита компьютерных систем, реализующих информационные технологии.	3.1 Классификация атак и методов взлома компьютерных систем. Атаки на уровне СУБД. Атаки на уровне операционных систем. Атаки на уровне сетевого программного обеспечения. 3.2 Защита операционных систем. Парольная защита и парольные взломщики. Криптографический протокол аутентификации Kerberos (Цербор).	2
10	Защита компьютерных систем, реализующих информационные технологии	Тема 3 Защита компьютерных систем, реализующих информационные технологии.	3.3 Защита от программ-шпионов. Защита от программных закладок. Защита от компьютерных вирусов и троянских программ. 3.4 Программные закладки и методы защиты от них. Троянские программы. Клавиатурные шпионы и методы защиты от них. Парольные взломщики. 3.5 Защита от ПЭМИН. Источники утечки информации по каналам ПЭМИН. Организация защиты информации в ИС от перехвата излучений и наводок.	2

11	Защита сетевых информационных технологий	Тема 4. Защита сетевых информационных технологий.	4.1 Проблемы защиты корпоративных компьютерных сетей. Сетевые утилиты и сканеры. Анализаторы протоколов и защита от них. Проблемы широковещательного режима компьютерных сетей. 4.2 Методы и средства защиты от удаленных сетевых атак. Особенности функционирования межсетевых экранов. Основные компоненты межсетевых экранов.	2
12	Защита сетевых информационных технологий	Тема 4. Защита сетевых информационных технологий.	4.3 Основные схемы сетевой защиты. Фильтрующий маршрутизатор. Экранированный шлюз. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты. 4.4 Межсетевые экраны, особенности функционирования и компоненты. Шлюзы сетевого уровня. Шлюзы прикладного уровня. Межсетевой экран на основе двупортового шлюза. 4.5 Межсетевой экран с экранированным шлюзом. Межсетевой экран с экранированной подсетью. Распределенные межсетевые экраны.	2
13	Защита сетевых информационных технологий	Тема 4. Защита сетевых информационных технологий.	Программные методы защиты корпоративных сетей. Защищенные сетевые протоколы. Протоколы SSL и SHTTP. SKIP - технология. SSL - протокол защиты соединения. 4.7 Логические архитектуры современных компьютерных сетей Модели классической архитектуры "клиент-сервер". Архитектура "клиент-сервер", основанная на WEB-технологии. 4.8 Модель комплексной оценки СЗИ. Методика оценки качества СЗИ на основе матрицы знаний. Использование лингвистической переменной для оценки качества СЗИ. Методика оценки с использованием профиля безопасности. Оценка качества защиты.	2
14	Управление безопасностью информации в автоматизированных системах	Тема 5. Управление безопасностью информации в автоматизированных системах.	5.1 Задачи управления безопасностью. Функции управления безопасностью. Структура подсистемы управления безопасностью. Система поддержки принятия решений по управлению безопасностью. 5.2 Источники угроз информационным технологиям в АСУ. Система управления безопасностью информации в АСУ, ее функции и задачи. Центр управления безопасностью в АСУ и его функциональные уровни.	2

15	Управление безопасностью информации в автоматизированных системах	Тема 5. Управление безопасностью информации в автоматизированных системах.	5.3 Система поддержки принятия решений по управлению безопасностью в АСУ. Принципы и методы защиты информации в АС. Структура монитора обращений. Политика безопасности и меры по ее реализации. 5.4 Методы идентификации и аутентификации. Проектирование систем защиты информации в АСУ. Классы защищенности АС от НСД. Классификация атак и методов взлома компьютерных систем.	2
16	Управление безопасностью информации в автоматизированных системах	Тема 5. Управление безопасностью информации в автоматизированных системах.	5.5 Принципы построения систем защиты информации в автоматизированных системах. Синтез структуры системы защиты информации. 5.6 Выбор методов идентификации и аутентификации в системе защиты. Выбор методов контроля доступа. Система стандартизации в области защиты информации. Заключение. Перспективы развития защищенных информационных технологий.	2
Итого за семестр:				32
Итого:				32

4.2 Содержание лабораторных занятий

№ занятия	Наименование раздела	Тема лабораторного занятия	Содержание лабораторного занятия (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов / часов в электронной форме
6 семестр				
1	Принцип защиты и обеспечения информационной безопасности современных информационных технологий	Лабораторная работа №1. Угрозы современным информационным технологиям.	Источники угроз информационным технологиям. Каналы утечки информации. Задачи защиты информационных технологий. Основные принципы защиты информации. Категории и уровни информационной безопасности.	2
2	Принцип защиты и обеспечения информационной безопасности современных информационных технологий	Лабораторная работа №1. Угрозы современным информационным технологиям.	Источники угроз информационным технологиям. Каналы утечки информации. Задачи защиты информационных технологий. Основные принципы защиты информации. Категории и уровни информационной безопасности.	2
3	Принцип защиты и обеспечения информационной безопасности современных информационных технологий	Лабораторная работа №1. Угрозы современным информационным технологиям.	Модели защиты информации. Управление доступом. Сравнительная характеристика матричных и потоковых моделей защиты информации.	2

4	Принцип защиты и обеспечения информационной безопасности современных информационных технологий	Лабораторная работа №1. Угрозы современным информационным технологиям.	Модели защиты информации. Управление доступом. Сравнительная характеристика матричных и потоковых моделей защиты информации.	2
5	Принципы шифрования информации	Лабораторная работа №2. Простые шифры и системы Цезаря.	Шифры перестановки. Шифры простой замены. Аффинная система Цезаря. Система Цезаря с ключевым словом.	2
6	Принципы шифрования информации	Лабораторная работа №2. Простые шифры и системы Цезаря.	Шифры перестановки. Шифры простой замены. Аффинная система Цезаря. Система Цезаря с ключевым словом.	2
7	Принципы шифрования информации	Лабораторная работа №3. Многоалфавитные шифры.	Система шифрования Вижинера. Двойной квадрат Уитстона. Одноразовые системы шифрования. Одноразовый шифрблокнот. Шифрование методом Вернама. Шифрование гаммированием. Методы генерации псевдослучайных последовательностей.	2
8	Принципы шифрования информации	Лабораторная работа №3. Многоалфавитные шифры.	Система шифрования Вижинера. Двойной квадрат Уитстона. Одноразовые системы шифрования. Одноразовый шифрблокнот. Шифрование методом Вернама. Шифрование гаммированием. Методы генерации псевдослучайных последовательностей.	2
9	Принципы шифрования информации	Лабораторная работа №4. Управление ключами в криптосистемах.	Асимметричная методология шифрования. Электронно-цифровая подпись. Усиленная аутентификация. Симметричные криптосистемы. Криптосистема DES. Принцип итерирования и конструкция Фейстеля. Основные режимы блочного шифрования. Стандарт шифрования данных DES. Цикл преобразования в криптосистеме DES.	2
10	Принципы шифрования информации	Лабораторная работа №4. Управление ключами в криптосистемах	Асимметричная методология шифрования. Электронно-цифровая подпись. Усиленная аутентификация. Симметричные криптосистемы. Криптосистема DES. Принцип итерирования и конструкция Фейстеля. Основные режимы блочного шифрования. Стандарт шифрования данных DES. Цикл преобразования в криптосистеме DES.	2
11	Принципы шифрования информации	Лабораторная работа №5. Современные блочные симметричные криптосистемы.	Комбинирование блочных алгоритмов. Алгоритм шифрования IDEA. Отечественный стандарт шифрования данных ГОСТ 28147-89. Сравнительная оценка симметричных криптосистем. Асимметричные криптосистемы. Односторонние функции. Проблемы факторизации и дискретного логарифмирования больших чисел.	2

12	Принципы шифрования информации	Лабораторная работа №5. Современные блочные симметричные криптосистемы.	Комбинирование блочных алгоритмов. Алгоритм шифрования IDEA. Отечественный стандарт шифрования данных ГОСТ 28147-89. Сравнительная оценка симметричных криптосистем. Асимметричные криптосистемы. Односторонние функции. Проблемы факторизации и дискретного логарифмирования больших чисел.	2
13	Защита компьютерных систем, реализующих информационные технологии	Лабораторная работа №7. Защита операционных систем. Парольная защита и парольные взломщики. Криптографический протокол аутентификации Kerberos (Цербор).	Защита от программ-шпионов. Защита от программных закладок. Защита от компьютерных вирусов и троянских программ.	2
14	Защита компьютерных систем, реализующих информационные технологии	Лабораторная работа №7. Защита операционных систем. Парольная защита и парольные взломщики. Криптографический протокол аутентификации Kerberos (Цербор).	Защита от программ-шпионов. Защита от программных закладок. Защита от компьютерных вирусов и троянских программ.	2
15	Защита компьютерных систем, реализующих информационные технологии	Лабораторная работа №7. Защита операционных систем. Парольная защита и парольные взломщики. Криптографический протокол аутентификации Kerberos (Цербор).	Программные закладки и методы защиты от них. Троянские программы. Клавиатурные шпионы и методы защиты от них. Парольные взломщики.	2
16	Защита компьютерных систем, реализующих информационные технологии	Лабораторная работа №7. Защита операционных систем. Парольная защита и парольные взломщики. Криптографический протокол аутентификации Kerberos (Цербор).	Программные закладки и методы защиты от них. Троянские программы. Клавиатурные шпионы и методы защиты от них. Парольные взломщики.	2
17	Защита сетевых информационных технологий	Лабораторная работа №8. Проблемы защиты корпоративных компьютерных сетей.	Сетевые утилиты и сканеры. Анализаторы протоколов и защита от них. Проблемы широковещательного режима компьютерных сетей. Методы и средства защиты от удаленных сетевых атак. Особенности функционирования межсетевых экранов. Основные компоненты межсетевых экранов.	2

18	Защита сетевых информационных технологий	Лабораторная работа №8. Проблемы защиты корпоративных компьютерных сетей.	Сетевые утилиты и сканеры. Анализаторы протоколов и защита от них. Проблемы широкополосного режима компьютерных сетей. Методы и средства защиты от удаленных сетевых атак. Особенности функционирования межсетевых экранов. Основные компоненты межсетевых экранов.	2
19	Защита сетевых информационных технологий	Лабораторная работа №8. Проблемы защиты корпоративных компьютерных сетей.	Основные схемы сетевой защиты. Фильтрующий маршрутизатор. Экранированный шлюз. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты. Программные методы защиты корпоративных сетей. Защищенные сетевые протоколы. Протоколы SSL и SHTTP. SKIP-технология. SSL-протокол защиты соединения. Логические архитектуры современных компьютерных сетей. Модели классической архитектуры "клиент-сервер". Архитектура "клиент-сервер", основанная на WEB-технологии.	2
20	Защита сетевых информационных технологий	Лабораторная работа №8. Проблемы защиты корпоративных компьютерных сетей.	Основные схемы сетевой защиты. Фильтрующий маршрутизатор. Экранированный шлюз. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты. Программные методы защиты корпоративных сетей. Защищенные сетевые протоколы. Протоколы SSL и SHTTP. SKIP-технология. SSL-протокол защиты соединения. Логические архитектуры современных компьютерных сетей. Модели классической архитектуры "клиент-сервер". Архитектура "клиент-сервер", основанная на WEB-технологии.	2
21	Управление безопасностью информации в автоматизированных системах	Лабораторная работа №9. Система поддержки принятия решений по управлению безопасностью в АСУ.	Принципы и методы защиты информации в АС. Структура монитора обращений. Политика безопасности и меры по ее реализации.	2
22	Управление безопасностью информации в автоматизированных системах	Лабораторная работа №9. Система поддержки принятия решений по управлению безопасностью в АСУ.	Принципы и методы защиты информации в АС. Структура монитора обращений. Политика безопасности и меры по ее реализации.	2
23	Управление безопасностью информации в автоматизированных системах	Лабораторная работа №9. Система поддержки принятия решений по управлению безопасностью в АСУ.	Методы идентификации и аутентификации.	2

24	Управление безопасностью информации в автоматизированных системах	Лабораторная работа №9. Система поддержки принятия решений по управлению безопасностью в АСУ.	Методы идентификации и аутентификации.	2
Итого за семестр:				48
Итого:				48

4.3 Содержание практических занятий

Учебные занятия не реализуются.

4.4. Содержание самостоятельной работы

Наименование раздела	Вид самостоятельной работы	Содержание самостоятельной работы (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов
6 семестр			
Принцип защиты и обеспечения информационной безопасности современных информационных технологий	Подготовка к лабораторным работам	Модели защиты информации. Управление доступом. Сравнительная характеристика матричных и потоковых моделей защиты информации.	4
Принципы шифрования информации	Подготовка к лабораторным работам	Криптосистема DES. Принцип итерирования и конструкция Фейстеля. Основные режимы блочного шифрования. Стандарт шифрования данных DES. Цикл преобразования в криптосистеме DES.	6
Принципы шифрования информации	Подготовка к зачету	Комбинирование блочных алгоритмов. Алгоритм шифрования IDEA. Отечественный стандарт шифрования данных ГОСТ 28147-89. Сравнительная оценка симметричных криптосистем. Асимметричные криптосистемы. Односторонние функции. Проблемы факторизации и дискретного логарифмирования больших чисел.	6
Защита компьютерных систем, реализующих информационные технологии	Подготовка к лабораторным работам	Защита от программ-шпионов. Защита от программных закладок. Защита от компьютерных вирусов и троянских программ.	4
Защита компьютерных систем, реализующих информационные технологии	Подготовка к зачету	Троянские программы. Клавиатурные шпионы и методы защиты от них. Парольные взломщики.	4

Защита сетевых информационных технологий	Подготовка к лабораторным работам	Программные методы защиты корпоративных сетей. Защищенные сетевые протоколы. Протоколы SSL и SHTTP. SKIP-технология. SSL-протокол защиты соединения. Логические архитектуры современных компьютерных сетей. Модели классической архитектуры "клиент-сервер". Архитектура "клиент-сервер", основанная на WEB-технологии.	3
Управление безопасностью информации в автоматизированных системах	Подготовка к лабораторным работам	Система поддержки принятия решений по управлению безопасностью в АСУ	4
Управление безопасностью информации в автоматизированных системах	Подготовка к зачету	Принципы и методы защиты информации в АС. Структура монитора обращений. Политика безопасности и меры по ее реализации. Методы идентификации и аутентификации.	2
Итого за семестр:			33
Итого:			33

5. Перечень учебной литературы и учебно-методического обеспечения по дисциплине (модулю)

№ п/п	Библиографическое описание	Ресурс НТБ СамГТУ (ЭБС СамГТУ, IPRbooks и т.д.)
Основная литература		
1	Прохорова, О.В. Информационная безопасность и защита информации : учебник / О. В. Прохорова; Самарский государственный технический университет, Самарский государственный архитектурно-строительный университет.- Самара, 2014.- 114 с.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu elib 4779	Электронный ресурс
2	Шаньгин, В.Ф. Защита компьютерной информации : Эффектив.методы и средства:Учеб.пособие / В. Ф. Шаньгин.- М., ДМК Пресс, 2008.- 542 с.	Электронный ресурс
Дополнительная литература		
3	Информационная безопасность и защита информации : Учеб.пособие / Ю.Ю.Громов,В.О.Драчев,О.Г.Иванова,Н.Г.Шахов.- Старый Оскол, ТНТ, 2010.- 383 с.	Электронный ресурс

Доступ обучающихся к ЭР НТБ СамГТУ (elib.samgtu.ru) осуществляется посредством электронной информационной образовательной среды университета и сайта НТБ СамГТУ по логину и паролю.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

При проведении лекционных занятий используется мультимедийное оборудование.

Организовано взаимодействие обучающегося и преподавателя с использованием электронной ин-формационной образовательной среды университета.

№ п/п	Наименование	Производитель	Способ распространения
1	Операционная система Windows 7	Microsoft (Зарубежный)	Лицензионное
2	Операционная система Astra Linux Special Edition	ГК Astra Linux (ООО «Рус-БИТех-Астра») (Отечественный)	Лицензионное
3	Kaspersky Endpoint Security 11.6.0.394	Лаборатория Касперского (Отечественный)	Лицензионное
4	OpenOffice 3.2	Apache Software Foundation (Зарубежный)	Свободно распространяемое
5	Средство просмотра PDF-файлов PDF24 10.0.10	Geek Software GmbH (Зарубежный)	Свободно распространяемое
6	Средство просмотра DJVU-файлов WinDjView 2.1	Андрей и Леонид Жеже-рун (Отечественный)	Свободно распространяемое

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем

№ п/п	Наименование	Краткое описание	Режим доступа
1	Поисковая система SciVerse	http://www.scopus.com	Ресурсы открытого доступа
2	Технические журналы «В мире науки»	http://journal.knigka.info/category/inworldsciences/	Ресурсы открытого доступа
3	КонсультантПлюс (правовые документы) - доступ с ПК в Медиацентре (ауд. 42)	http://www.consultant.ru/	Российские базы данных ограниченного доступа
4	eLIBRARY.ru	http://www.eLIBRARY.ru/	Российские базы данных ограниченного доступа

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Лекционные занятия

Учебная аудитория № 113 для проведения занятий лекционного типа, практических занятий и занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Технические средства обучения, служащие для представления учебной информации большой аудитории, набор демонстрационного оборудования: телевизор, кабель HDMI, переносной ноутбук с возможностью

подключения к сети «Интернет» и с доступом в электронную информационно-образовательную среду вуза.

Пакет прикладных программных продуктов:

- Операционная система Windows 10
- Kaspersky Endpoint Security 11.6.0.394
- Комплекс офисных приложений OpenOffice 3.2
- Средство просмотра PDF-файлов PDF24 10.0.10
- Средство просмотра DJVU-файлов WinDjView 2.

Практические занятия null

Лабораторные занятия

Лаборатория № 114 в области технологий обеспечения информационной безопасности и защищенных информационных систем. Учебная лаборатория для проведения занятий лекционного типа, семинарского типа, лабораторных работ, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория оснащена средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации:

Многоканальный комплекс обнаружения радиоизлучающих средств и радиомониторинга "Крона Про"и СПО "Филин Ультра"

- устройство обнаружения скрытых видеокамер "Амулет"
- антенный измерительный комплекс "АИК 1-40А"
- диктофон RR-US510
- комплект антенн измерительных АИ 5-0 и АИ 3-2, анализатор спектра GSP-827
- аппаратура имитации сигналов «Аврора-2»
- портативный измеритель частоты и мощности «MFP-8000»
- поисковый приемник радиосигналов «Скорпион»
- программно-аппаратный комплекс для проведения специсследований «Навигатор-ПЗГ»
- программно-аппаратный комплекс для проведения акустических и виброакустических измерений «Спрут-7А»
- многофункциональный поисковый прибор ST-031 «Пиранья»

18

- специальный сканирующий приемник AR-3000А и ПО «Филин»
- портативный нелинейный локатор SP-61 «Катран»
- генератор шума «ГРОМ-ЗИ-4»
- прибор виброакустической защиты «SI-3001»,
- устройство предотвращения утечки информации по каналам систем мобильной связи

МОЗАИКА

- контроллер телефонной линии КТЛ-400.

Пакет прикладных программных продуктов:

- Операционная система Windows 10
- Kaspersky Endpoint Security 11.6.0.394
- Комплекс офисных приложений OpenOffice 3.2
- Средство просмотра PDF-файлов PDF24 10.0.10

Самостоятельная работа

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде СамГТУ:

- читальный зал НТБ СамГТУ (ауд. 200 корпус № 8; ауд. 125 корпус № 1; ауд. 41, 31, 34, 35
Главный корпус библиотеки, ауд. 83а, 414, 416, 0209 АСА СамГТУ; ауд. 401 корпус №10);

- лаборатория № 107 (компьютерный класс) для проведения занятий лекционного типа, практических занятий и занятий семинарского типа, лабораторных работ, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Пакет прикладных программных продуктов:

- Операционная система Windows 10

- Операционная система Astra Linux Special Edition
- Kaspersky Endpoint Security 11.6.0.394
- XSpider Education
- Positive Technologies Application Firewall Education
- Комплекс офисных приложений OpenOffice 3.2
- Средство просмотра PDF-файлов PDF24 10.0.10

9. Методические материалы

Методические рекомендации при работе на лекции

До лекции студент должен просмотреть учебно-методическую и научную литературу по теме лекции с тем, чтобы иметь представление о проблемах, которые будут разбираться в лекции.

Перед началом лекции обучающимся сообщается тема лекции, план, вопросы, подлежащие рассмотрению, доводятся основные литературные источники. Весь учебный материал, сообщаемый преподавателем, должен не просто прослушиваться. Он должен быть активно воспринят, т.е. услышан, осмыслен, понят, зафиксирован на бумаге и закреплен в памяти. Приступая к слушанию нового учебного материала, полезно мысленно установить его связь с ранее изученным. Следя за техникой чтения лекции (акцент на существенном, повышение тона, изменение ритма, пауза и т.п.), необходимо вслед за преподавателем уметь выделять основные категории, законы и определять их содержание, проблемы, предполагать их возможные решения, доказательства и выводы. Осуществляя такую работу, можно значительно облегчить себе понимание учебного материала, его конспектирование и дальнейшее изучение.

Конспектирование лекции позволяет обработать, систематизировать и лучше сохранить полученную информацию с тем, чтобы в будущем можно было восстановить в памяти основные, содержательные моменты. Типичная ошибка, совершаемая обучающимся, дословное конспектирование речи преподавателя. Как правило, при записи «слово в слово» не остается времени на обдумывание, анализ и синтез информации. Отбирая нужную информацию, главные мысли, проблемы, решения и выводы, необходимо сокращать текст, строить его таким образом, чтобы потом можно было легко в нем разобраться. Желательно оставить в рабочих конспектах поля, на которых можно будет делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. С окончанием лекции работа над конспектом не может считаться завершённой. Нужно еще восстановить отдельные места, проверить, все ли понятно, уточнить что-то на консультации и т.п. с тем, чтобы конспект мог быть использован в процессе подготовки к практическим занятиям, зачету, экзамену. Конспект лекции – незаменимый учебный документ, необходимый для самостоятельной работы.

Методические рекомендации при работе на лабораторном занятии

Проведение лабораторной работы делится на две условные части: теоретическую и практическую.

Необходимыми структурными элементами занятия являются проведение лабораторной работы, проверка усвоенного материала, включающая обсуждение теоретических основ выполняемой работы.

Перед лабораторной работой, как правило, проводится технико-теоретический инструктаж по использованию необходимого оборудования. Преподаватель корректирует деятельность обучающегося в процессе выполнения работы (при необходимости). После завершения лабораторной работы подводятся итоги, обсуждаются результаты деятельности.

Возможны следующие формы организации лабораторных работ: фронтальная, групповая и индивидуальная. При фронтальной форме выполняется одна и та же работа (при этом возможны различные варианты заданий). При групповой форме работа выполняется группой (командой). При индивидуальной форме обучающимися выполняются индивидуальные работы.

По каждой лабораторной работе имеются методические указания по их выполнению, включающие необходимый теоретический и практический материал, содержащие элементы и последовательную инструкцию по проведению выбранной работы, индивидуальные варианты заданий, требования и форму отчётности по данной работе.

Методические рекомендации по выполнению самостоятельной работы

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению с учетом потребностей и возможностей обучающегося.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.

Самостоятельная работа реализуется:

- непосредственно в процессе аудиторных занятий;
- на лекциях, практических занятиях;
- в контакте с преподавателем вне рамок расписания;
- на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.;
- в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем.

10. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств представлен в приложении № 1.

**Фонд оценочных средств
по дисциплине
Б1.В.01.ДВ.03.02 «Защищенные информационные технологии»**

Код и направление подготовки (специальность)	10.03.01 Информационная безопасность
Направленность (профиль)	Комплексная защита объектов информатизации (в промышленности)
Квалификация	Бакалавр
Форма обучения	Очная
Год начала подготовки	2020
Институт / факультет	Институт автоматизации и информационных технологий
Выпускающая кафедра	кафедра "Электронные системы и информационная безопасность"
Кафедра-разработчик	кафедра "Электронные системы и информационная безопасность"
Объем дисциплины, ч. / з.е.	144 / 4
Форма контроля (промежуточная аттестация)	Экзамен

**Перечень планируемых результатов обучения по дисциплине (модулю),
соотнесенных с планируемыми результатами освоения образовательной
программы**

Код и наименование компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Общепрофессиональные компетенции	
ОПК-4 способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Владеть навыками проектирования архитектуры системы защиты информации, для обеспечения информационной безопасности объекта, В(ПК-1) -1
	Знать как провести предварительный технико-экономический анализ и обоснование проектных решений по обеспечению информационной безопасности, З(ОПК-4) -1;
	Уметь понимать сущность и значение информации в развитии современного общества, У(ОПК-4) -1;
Профессиональные компетенции	
ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты	Владеть - навыками администрирования подсистем информационной безопасности объекта защиты; - навыками проектирования архитектуры системы защиты информации, для обеспечения информационной безопасности объекта, В(ПК-3) -1
	Знать основы администрирования подсистемы информационной безопасности, З(ПК-3) -1;
	Уметь быстро разобраться в протоколах администрирования подсистемы информационной безопасности объекта защиты, У(ПК-3) -1;

Матрица соответствия оценочных средств запланированным результатам обучения

Код и наименование компетенции	Результаты обучения	Оценочные средства	Текущий контроль успеваемости	Промежуточная аттестация
Принцип защиты и обеспечения информационной безопасности современных информационных технологий				
ОПК-4 способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Уметь понимать сущность и значение информации в развитии современного общества, У(ОПК-4) -1;	Отчет по лабораторной работе	Да	Нет

	Владеть навыками проектирования архитектуры системы защиты информации, для обеспечения информационной безопасности объекта, В(ПК-1) -1	Отчет по лабораторной работе	Да	Да
	Знать как провести предварительный технико-экономический анализ и обоснование проектных решений по обеспечению информационной безопасности, З(ОПК-4) -1;	Вопросы к зачету	Нет	Да
ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты	Знать основы администрирования подсистемы информационной безопасности, З(ПК-3) -1;	отчет по лабораторным работам	Да	Нет
		Вопросы к зачету	Нет	Да
	Уметь быстро разобраться в протоколах администрирования подсистемы информационной безопасности объекта защиты, У(ПК-3) -1;	отчет по лабораторным работам	Да	Нет
	Владеть - навыками администрирования подсистем информационной безопасности объекта защиты; - навыками проектирования архитектуры системы защиты информации, для обеспечения информационной безопасности объекта, В(ПК-3) -1	отчет по лабораторным работам	Да	Нет
Принципы шифрования информации				
ОПК-4 способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Знать как провести предварительный технико-экономический анализ и обоснование проектных решений по обеспечению информационной безопасности, З(ОПК-4) -1;	отчет по лабораторным работам	Да	Нет
		Вопросы к зачету	Нет	Да
	Владеть навыками проектирования архитектуры системы защиты информации, для обеспечения информационной безопасности объекта, В(ПК-1) -1	отчет по лабораторным работам	Да	Нет
	Уметь понимать сущность и значение информации в развитии современного общества, У(ОПК-4) -1;	отчет по лабораторным работам	Да	Нет
ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты	Уметь быстро разобраться в протоколах администрирования подсистемы информационной безопасности объекта защиты, У(ПК-3) -1;	отчет по лабораторным работам	Да	Нет
	Владеть - навыками администрирования подсистем информационной безопасности объекта защиты; - навыками проектирования архитектуры системы защиты информации, для обеспечения информационной безопасности объекта, В(ПК-3) -1	отчет по лабораторным работам	Да	Нет

	Знать основы администрирования подсистемы информационной безопасности, З(ПК-3) -1;	Вопросы к зачету	Нет	Да
		отчет по лабораторным работам	Да	Нет
Защита компьютерных систем, реализующих информационные технологии				
ОПК-4 способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Владеть навыками проектирования архитектуры системы защиты информации, для обеспечения информационной безопасности объекта, В(ПК-1) -1	отчет по лабораторным работам	Да	Нет
	Уметь понимать сущность и значение информации в развитии современного общества, У(ОПК-4) -1;	отчет по лабораторным работам	Да	Нет
	Знать как провести предварительный технико-экономический анализ и обоснование проектных решений по обеспечению информационной безопасности, З(ОПК-4) -1;	Вопросы к зачету	Нет	Да
		отчет по лабораторным работам	Да	Нет
ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты	Уметь быстро разобраться в протоколах администрирования подсистемы информационной безопасности объекта защиты, У(ПК-3) -1;	отчет по лабораторным работам	Да	Нет
		Владеть - навыками администрирования подсистем информационной безопасности объекта защиты; - навыками проектирования архитектуры системы защиты информации, для обеспечения информационной безопасности объекта, В(ПК-3) -1	отчет по лабораторным работам	Да
	Знать основы администрирования подсистемы информационной безопасности, З(ПК-3) -1;	Вопросы к зачету	Нет	Да
		отчет по лабораторным работам	Да	Нет
Защита сетевых информационных технологий				
ОПК-4 способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Уметь понимать сущность и значение информации в развитии современного общества, У(ОПК-4) -1;	отчет по лабораторным работам	Да	Нет
	Знать как провести предварительный технико-экономический анализ и обоснование проектных решений по обеспечению информационной безопасности, З(ОПК-4) -1;	Вопросы к зачету	Нет	Да
	Владеть навыками проектирования архитектуры системы защиты информации, для обеспечения информационной безопасности объекта, В(ПК-1) -1	отчет по лабораторным работам	Да	Нет

ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты	Владеть - навыками администрирования подсистем информационной безопасности объекта защиты; - навыками проектирования архитектуры системы защиты информации, для обеспечения информационной безопасности объекта, В(ПК-3) -1	отчет по лабораторным работам	Нет	Нет	
	Знать основы администрирования подсистемы информационной безопасности, З(ПК-3) -1;	Вопросы к зачету	Нет	Да	
	Уметь быстро разобраться в протоколах администрирования подсистемы информационной безопасности объекта защиты, У(ПК-3) -1;	отчет по лабораторным работам	Да	Нет	
Управление безопасностью информации в автоматизированных системах					
ОПК-4 способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Уметь понимать сущность и значение информации в развитии современного общества, У(ОПК-4) -1;	отчет по лабораторным работам	Да	Нет	
	Владеть навыками проектирования архитектуры системы защиты информации, для обеспечения информационной безопасности объекта, В(ПК-1) -1	отчет по лабораторным работам	Да	Нет	
		Вопросы к зачету	Нет	Да	
	Знать как провести предварительный технико-экономический анализ и обоснование проектных решений по обеспечению информационной безопасности, З(ОПК-4) -1;	отчет по лабораторным работам	Да	Нет	
		Вопросы к зачету	Нет	Да	
	ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты	Знать основы администрирования подсистемы информационной безопасности, З(ПК-3) -1;	отчет по лабораторным работам	Да	Нет
Вопросы к зачету			Нет	Да	
Владеть - навыками администрирования подсистем информационной безопасности объекта защиты; - навыками проектирования архитектуры системы защиты информации, для обеспечения информационной безопасности объекта, В(ПК-3) -1		отчет по лабораторным работам	Да	Нет	
		Уметь быстро разобраться в протоколах администрирования подсистемы информационной безопасности объекта защиты, У(ПК-3) -1;	отчет по лабораторным работам	Да	Нет

Типовые контрольные задания или иные материалы для оценки знаний, умений, навыков, характеризующих этапы формирования компетенций в процессе освоения ОПОП

Перечень подлежащих оценке результатов обучения (показателей проявления компетенций: владений, умений, знаний) при использовании предусмотренных рабочей программой дисциплины оценочных средств представлены в табл. 2.

3.1. Перечень вопросов для промежуточной аттестации (зачет с оценкой)

1. Угрозы современным информационным технологиям. Источники угроз информационным технологиям. Каналы утечки информации. Задачи защиты информационных технологий. Основные принципы защиты информации. Категории и уровни информационной безопасности.
2. Компьютерные преступления. Законодательная база по информационным технологиям. Современная классификация компьютерных преступлений Минимальный список нарушений в области компьютерных преступлений. Законодательная база по информационным технологиям. Ответственность за компьютерные преступления.
3. Принципы защиты информации и информационных технологий. Оранжевая книга и общие принципы защиты информации. Политика безопасности и ее функции.
4. Теоретические основы защиты информации. Типы и модели политики безопасности. Современные исследования в области защиты информации.
5. Модели защиты информации. Управление доступом. Сравнительная характеристика матричных и потоковых моделей защиты информации.
6. Принципы криптографической защиты информации. Структуры криптографического преобразования информации. Требования к шифрам, используемым для криптографической защиты информации. Шифры традиционных симметричных криптосистем.
7. Криптоаналитические атаки и их классификация. Классификация криптоаналитических атак. Стойкость криптоалгоритма. Причины успешных атак на криптоалгоритмы и методы борьбы с ними.
8. Простые шифры и системы Цезаря. Шифры перестановки. Шифры простой замены. Аффинная система Цезаря. Система Цезаря с ключевым словом.
9. Биграмные шифры и шифры сложной замены. Шифрующие таблицы Трисемуса. Биграмный шифр Плейфейра. Криптосистема Хилла.
10. Многоалфавитные шифры. Система шифрования Вижинера. Двойной квадрат Уитстона.
11. Одноразовые системы шифрования. Одноразовый шифр-блокнот. Шифрование методом Вернама. Шифрование гаммированием. Методы генерации псевдослучайных последовательностей.
12. Управление ключами в криптосистемах. Асимметричная методология шифрования. Электронно - цифровая подпись. Усиленная аутентификация.
13. Современные криптосистемы. Классификация современных алгоритмов шифрования. Блочные и поточные алгоритмы. Симметричная и асимметричная методологии. Методы реализации криптосистем.
14. Симметричные криптосистемы. Криптосистема DES. Принцип итерирования и конструкция Фейстеля. Основные режимы блочного шифрования. Стандарт шифрования данных DES. Цикл преобразования в криптосистеме DES.
15. Современные блочные симметричные криптосистемы. Комбинирование блочных алгоритмов. Алгоритм шифрования IDEA. Отечественный стандарт шифрования данных ГОСТ 28147-89. Сравнительная оценка симметричных криптосистем.

16. Асимметричные криптосистемы. Односторонние функции. Проблемы факторизации и дискретного логарифмирования больших чисел.
17. Стандарт асимметричного шифрования RSA. Алгоритмические преобразования в системе RSA. Процессы шифрования и расшифровывания. Криптостойкость и быстродействие системы RSA.
18. Распространенные асимметричные и комбинированные схемы шифрования. Схема шифрования Полига - Хелмана. Схема шифрования Эль Гамала. Комбинированная схема шифрования открытым и закрытым ключами. Система SSL.
19. Проблема аутентификации данных и электронно-цифровая подпись. Однонаправленные хеш-функции. Схемы формирования ЭЦП (алгоритмы RSA, EGSA, DSA). Отечественный стандарт ЭЦП.
20. Идентификация и проверка подлинности. Идентификация и аутентификация пользователя. Взаимная проверка подлинности. Протоколы идентификации с нулевой передачей знаний.
21. Управление криптографическими ключами. Генерация и хранение ключей. Распределение ключей.
22. Новые направления в шифровании информации. "Шарады" с временным замком. Квантовая криптография. Компьютерная стеганография. Электронные водяные знаки.
23. Классификация атак и методов взлома компьютерных систем. Атаки на уровне СУБД. Атаки на уровне операционных систем. Атаки на уровне сетевого программного обеспечения.
24. Защита операционных систем. Парольная защита и парольные взломщики. Криптографический протокол аутентификации Kerberos (Цербер).
25. Защита от программ-шпионов. Защита от программных закладок. Защита от компьютерных вирусов и троянских программ.
26. Программные закладки и методы защиты от них. Троянские программы. Клавиатурные шпионы и методы защиты от них. Парольные взломщики.
27. Защита от ПЭМИН. Источники утечки информации по каналам ПЭМИН. Организация защиты информации в ИС от перехвата излучений и наводок.
28. Проблемы защиты корпоративных компьютерных сетей. Сетевые утилиты и сканеры. Анализаторы протоколов и защита от них. Проблемы широковещательного режима компьютерных сетей.
29. Методы и средства защиты от удаленных сетевых атак. Особенности функционирования межсетевых экранов. Основные компоненты межсетевых экранов.
30. Основные схемы сетевой защиты. Фильтрующий маршрутизатор. Экранированный шлюз. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты.
31. Межсетевые экраны, особенности функционирования и компоненты. Шлюзы сетевого уровня. Шлюзы прикладного уровня. Межсетевой экран на основе двухпортового шлюза.
32. Межсетевой экран с экранированным шлюзом. Межсетевой экран с экранированной подсетью. Распределенные межсетевые экраны.
33. Программные методы защиты корпоративных сетей. Защищенные сетевые протоколы. Протоколы SSL и SHTTP. SKIP – технология. SSL – протокол защиты соединения.
34. Логические архитектуры современных компьютерных сетей.
35. Модели классической архитектуры "клиент-сервер". Архитектура "клиент-сервер", основанная на WEB-технологии.
36. Модель комплексной оценки СЗИ. Методика оценки качества СЗИ на основе матрицы знаний. Использование лингвистической переменной для оценки качества СЗИ. Методика оценки с использованием профиля безопасности. Оценка качества защиты.

37. Задачи управления безопасностью. Функции управления безопасностью. Структура подсистемы управления безопасностью. Система поддержки принятия решений по управлению безопасностью.
38. Источники угроз информационным технологиям в АСУ. Система управления безопасностью информации в АСУ, ее функции и задачи. Центр управления безопасностью в АСУ и его функциональные уровни.
39. Система поддержки принятия решений по управлению безопасностью в АСУ. Принципы и методы защиты информации в АС. Структура монитора обращений. Политика безопасности и меры по ее реализации.
40. Методы идентификации и аутентификации. Проектирование систем защиты информации в АСУ. Классы защищенности АС от НСД. Классификация атак и методов взлома компьютерных систем.
41. Принципы построения систем защиты информации в автоматизированных системах. Синтез структуры системы защиты информации.
42. Выбор методов идентификации и аутентификации в системе защиты. Выбор методов контроля доступа. Система стандартизации в области защиты информации.

Примерная структура билета на экзамен



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ»

Кафедра «Электронные системы и информационная безопасность»

по дисциплине

Защищенные информационные технологии

(наименование дисциплины)

Направление подготовки	10.03.01	Институт	АИТ	Семестр	6
	(шифр)	(наименование института)			(номер)

БИЛЕТ № 1

1. Угрозы современным информационным технологиям. Источники угроз информационным технологиям. Каналы утечки информации. Задачи защиты информационных технологий. Основные принципы защиты информации. Категории и уровни информационной безопасности.
2. Компьютерные преступления. Законодательная база по информационным технологиям. Современная классификация компьютерных преступлений Минимальный список нарушений в области компьютерных преступлений. Законодательная база по информационным технологиям. Ответственность за компьютерные преступления.

Составитель:

Заведующий кафедрой

_____ профессор Карпова Н.Е.

_____ Скобелев П.О.

«__» _____ 20__ года

«__» _____ 20__ года

Типовые контрольные задания или иные материалы для оценки знаний, умений, навыков, характеризующих этапы формирования компетенций в процессе освоения ОПОП

Перечень подлежащих оценке результатов обучения (показателей проявления компетенций: владений, умений, знаний) при использовании предусмотренных рабочей программой дисциплины оценочных средств представлены в табл. 2.

3.1. Перечень вопросов для промежуточной аттестации (зачет с оценкой)

1. Угрозы современным информационным технологиям. Источники угроз информационным технологиям. Каналы утечки информации. Задачи защиты информационных технологий. Основные принципы защиты информации. Категории и уровни информационной безопасности.
2. Компьютерные преступления. Законодательная база по информационным технологиям. Современная классификация компьютерных преступлений Минимальный список нарушений в области компьютерных преступлений. Законодательная база по информационным технологиям. Ответственность за компьютерные преступления.
3. Принципы защиты информации и информационных технологий. Оранжевая книга и общие принципы защиты информации. Политика безопасности и ее функции.
4. Теоретические основы защиты информации. Типы и модели политики безопасности. Современные исследования в области защиты информации.
5. Модели защиты информации. Управление доступом. Сравнительная характеристика матричных и потоковых моделей защиты информации.
6. Принципы криптографической защиты информации. Структуры криптографического преобразования информации. Требования к шифрам, используемым для криптографической защиты информации. Шифры традиционных симметричных криптосистем.
7. Криптоаналитические атаки и их классификация. Классификация криптоаналитических атак. Стойкость криптоалгоритма. Причины успешных атак на криптоалгоритмы и методы борьбы с ними.
8. Простые шифры и системы Цезаря. Шифры перестановки. Шифры простой замены. Аффинная система Цезаря. Система Цезаря с ключевым словом.
9. Биграмные шифры и шифры сложной замены. Шифрующие таблицы Трисемуса. Биграмный шифр Плейфейра. Криптосистема Хилла.
10. Многоалфавитные шифры. Система шифрования Вижинера. Двойной квадрат Уитстона.
11. Одноразовые системы шифрования. Одноразовый шифр-блокнот. Шифрование методом Вернама. Шифрование гаммированием. Методы генерации псевдослучайных последовательностей.
12. Управление ключами в криптосистемах. Асимметричная методология шифрования. Электронно - цифровая подпись. Усиленная аутентификация.
13. Современные криптосистемы. Классификация современных алгоритмов шифрования. Блочные и поточные алгоритмы. Симметричная и асимметричная методологии. Методы реализации криптосистем.
14. Симметричные криптосистемы. Криптосистема DES. Принцип итерирования и конструкция Фейстеля. Основные режимы блочного шифрования. Стандарт шифрования данных DES. Цикл преобразования в криптосистеме DES.
15. Современные блочные симметричные криптосистемы. Комбинирование блочных алгоритмов. Алгоритм шифрования IDEA. Отечественный стандарт шифрования данных ГОСТ 28147-89. Сравнительная оценка симметричных криптосистем.

16. Асимметричные криптосистемы. Односторонние функции. Проблемы факторизации и дискретного логарифмирования больших чисел.
17. Стандарт асимметричного шифрования RSA. Алгоритмические преобразования в системе RSA. Процессы шифрования и расшифровывания. Криптостойкость и быстродействие системы RSA.
18. Распространенные асимметричные и комбинированные схемы шифрования. Схема шифрования Полига - Хелмана. Схема шифрования Эль Гамала. Комбинированная схема шифрования открытым и закрытым ключами. Система SSL.
19. Проблема аутентификации данных и электронно-цифровая подпись. Однонаправленные хеш-функции. Схемы формирования ЭЦП (алгоритмы RSA, EGSA, DSA). Отечественный стандарт ЭЦП.
20. Идентификация и проверка подлинности. Идентификация и аутентификация пользователя. Взаимная проверка подлинности. Протоколы идентификации с нулевой передачей знаний.
21. Управление криптографическими ключами. Генерация и хранение ключей. Распределение ключей.
22. Новые направления в шифровании информации. "Шарады" с временным замком. Квантовая криптография. Компьютерная стеганография. Электронные водяные знаки.
23. Классификация атак и методов взлома компьютерных систем. Атаки на уровне СУБД. Атаки на уровне операционных систем. Атаки на уровне сетевого программного обеспечения.
24. Защита операционных систем. Парольная защита и парольные взломщики. Криптографический протокол аутентификации Kerberos (Цербер).
25. Защита от программ-шпионов. Защита от программных закладок. Защита от компьютерных вирусов и троянских программ.
26. Программные закладки и методы защиты от них. Троянские программы. Клавиатурные шпионы и методы защиты от них. Парольные взломщики.
27. Защита от ПЭМИН. Источники утечки информации по каналам ПЭМИН. Организация защиты информации в ИС от перехвата излучений и наводок.
28. Проблемы защиты корпоративных компьютерных сетей. Сетевые утилиты и сканеры. Анализаторы протоколов и защита от них. Проблемы широковещательного режима компьютерных сетей.
29. Методы и средства защиты от удаленных сетевых атак. Особенности функционирования межсетевых экранов. Основные компоненты межсетевых экранов.
30. Основные схемы сетевой защиты. Фильтрующий маршрутизатор. Экранированный шлюз. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты.
31. Межсетевые экраны, особенности функционирования и компоненты. Шлюзы сетевого уровня. Шлюзы прикладного уровня. Межсетевой экран на основе двупортового шлюза.
32. Межсетевой экран с экранированным шлюзом. Межсетевой экран с экранированной подсетью. Распределенные межсетевые экраны.
33. Программные методы защиты корпоративных сетей. Защищенные сетевые протоколы. Протоколы SSL и SHTTP. SKIP – технология. SSL – протокол защиты соединения.
34. Логические архитектуры современных компьютерных сетей.
35. Модели классической архитектуры "клиент-сервер". Архитектура "клиент-сервер", основанная на WEB-технологии.
36. Модель комплексной оценки СЗИ. Методика оценки качества СЗИ на основе матрицы знаний. Использование лингвистической переменной для оценки качества СЗИ. Методика оценки с использованием профиля безопасности. Оценка качества защиты.

37. Задачи управления безопасностью. Функции управления безопасностью. Структура подсистемы управления безопасностью. Система поддержки принятия решений по управлению безопасностью.
38. Источники угроз информационным технологиям в АСУ. Система управления безопасностью информации в АСУ, ее функции и задачи. Центр управления безопасностью в АСУ и его функциональные уровни.
39. Система поддержки принятия решений по управлению безопасностью в АСУ. Принципы и методы защиты информации в АС. Структура монитора обращений. Политика безопасности и меры по ее реализации.
40. Методы идентификации и аутентификации. Проектирование систем защиты информации в АСУ. Классы защищенности АС от НСД. Классификация атак и методов взлома компьютерных систем.
41. Принципы построения систем защиты информации в автоматизированных системах. Синтез структуры системы защиты информации.
42. Выбор методов идентификации и аутентификации в системе защиты. Выбор методов контроля доступа. Система стандартизации в области защиты информации.

Примерная структура билета на экзамен



МИНОБРНАУКИ РОССИИ
 Федеральное государственное бюджетное образовательное
 учреждение высшего образования
 «САМАРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
 УНИВЕРСИТЕТ»

Кафедра «Электронные системы и информационная безопасность»

по дисциплине

Защищенные информационные технологии

(наименование дисциплины)

Направление подготовки	10.03.01	Институт	АИТ	Семестр	6
	(шифр)	(наименование института)			(номер)

БИЛЕТ № 1

1. Угрозы современным информационным технологиям. Источники угроз информационным технологиям. Каналы утечки информации. Задачи защиты информационных технологий. Основные принципы защиты информации. Категории и уровни информационной безопасности.
2. Компьютерные преступления. Законодательная база по информационным технологиям. Современная классификация компьютерных преступлений Минимальный список нарушений в области компьютерных преступлений. Законодательная база по информационным технологиям. Ответственность за компьютерные преступления.

Составитель:

Заведующий кафедрой

_____ профессор Карпова Н.Е.

_____ Скобелев П.О.

«__» _____ 20__ года

«__» _____ 20__ года