Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Дальневосточный государственный университет путей сообщения"
(ДВГУПС)
Факультет среднего профессионального образования –
Хабаровский техникум железнодорожного транспорта

УТВЕРЖДАЮ
И.о.декана ФСПО - ХТЖТ
_____Д.Н. Никитин
«_21__» ___мая_____2021 г

РАБОЧАЯ ПРОГРАММА

дисциплины ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Для специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Профиль: -

Составитель(и): Преподаватель Касьяненко А.Ю.

Обсуждена на заседании ПЦК Информационная безопасность автоматизированных систем

Протокол от « 20 » мая 2021 г. № 9

Методист _____Л.В. Петрова

г. Хабаровск
2021 г.

ЛИСТ ДОПОЛНЕНИЙ И ИЗМЕНЕНИЙ (АКТУАЛИЗАЦИИ)

в рабочую программу ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

наименование структурного элемента ОПОП

10.02.05 Обеспечение информационной безопасности автоматизированных систем

с указанием кода направления подготовки и профиля

На основании

решения заседания кафедры (ПЦК) **Информационная безопасность автоматизированных систем**

полное наименование кафедры (ПЦК)

"26 " мая 2022 г., протокол № 9

на 2022 / 2023 учебный год внесены изменения:

№ / наименование раздела	Новая редакция
	Изменений нет

Заведующий кафедрой (председатель ПЦК)

_____А.Ю. Касьяненко

ЛИСТ ДОПОЛНЕНИЙ И ИЗМЕНЕНИЙ (АКТУАЛИЗАЦИИ)

в рабочую программу ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

наименование структурного элемента ОПОП

10.02.05 Обеспечение информационной безопасности автоматизированных систем

с указанием кода направления подготовки и профиля

На основании

решения заседания кафедры (ПЦК) **Информационная безопасность автоматизированных систем**

полное наименование кафедры (ПЦК)

"26 " мая 2023 г., протокол № 9

на 2023 / 2024 учебный год внесены изменения:

№ / наименование раздела	Новая редакция
	Изменений нет

Заведующий кафедрой (председатель ПЦК)

_____А.Ю. Касьяненко

Рабочая программа дисциплины ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

разработана в соответствии с ФГОС, утвержденным приказом Министерства образования и науки Российской Федерации от 09.12.2016 г. № 1553

Квалификация **Техник по защите информации**

Форма обучения **очная**

ОБЪЕМ ДИСЦИПЛИНЫ (МДК, ПМ) В ЧАСАХ С УКАЗАНИЕМ ОБЯЗАТЕЛЬНОЙ И МАКСИМАЛЬНОЙ НАГРУЗКИ ОБУЧАЮЩИХСЯ

Общая трудоемкость **931 ЧАС**

Часов по учебному плану 931

Виды контроля в семестрах:
Дифференцированный зачет: 4
Другие формы промежуточной аттестации: 4
Зачет: 5
Курсовой проект 6
Экзамен: 5, 6
Экзамен квалификационный: 6

Распределение часов дисциплины (МДК, ПМ) по семестрам (курсам)

Семестр (<Курс>.<Семестр на курсе>)	4 (2.2)		5 (3.1)		6 (3.2)		Итого	
Недель	14 2/3 (9)		7 (9)		12 (4)			
Вид занятий	УП	РПД	УП	РПД	УП	РПД	УП	РПД
МДК 02.01								
Лекции, уроки	16	16	46	46	46	46	108	108
Практические занятия	14	14	24	24	28	28	66	66
Самостоятельная работа					26	26	26	26
Лабораторные занятия					16	16	16	16
Курсовой проект					30	30	30	30
Консультации					6	6	6	6
Промежуточная аттестация (экзамен)					8	8	8	8
Итого	30	30	70	70	160	160	260	260
МДК 02.02								
Лекции, уроки	42	42	28	28			70	70
Практические занятия	18	18	15	15			33	33
Лабораторные занятия			6	6			6	6
Консультации			6	6			6	6
Промежуточная аттестация (экзамен)			8	8			8	8
Итого	60	60	63	63			123	123
Учебная практика по ПМ.02, 2 нед*								
Самостоятельная работа	72	72					72	72
Производственная практика по ПМ.02, 13 нед*								
Самостоятельная работа	252	252	216	216			468	468
Промежуточная аттестация (экзамен квалификационный)					8	8	8	8
Итого	414	414	349	349	168	168	931	931

*Программа практики приведена в отдельном документе

МДК.02.01 «*Программные и программно-аппаратные средства защиты информации*»

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МДК, ПМ)	
1.1	Предмет и задачи программно-аппаратной защиты информации. Стандарты безопасности. Защищенная автоматизированная система. Дестабилизирующее воздействие на объекты защиты. Принципы программно-аппаратной защиты информации от несанкционированного доступа. Основы защиты автономных автоматизированных систем. Защита программ от излучения. Вредоносное программное обеспечение. Защита программ и данных от несанкционированного копирования. Защита информации на машинных носителях. Аппаратные средства идентификации и аутентификации пользователей. Системы обнаружения атак и вторжений. Основы построения защищенных сетей. Средства организации VPN. Обеспечение безопасности межсетевого взаимодействия. Защита информации в базах данных. Мониторинг систем защиты. Изучение мер защиты информации в информационных системах. Изучение современных программно-аппаратных комплексов.

2. МЕСТО ДИСЦИПЛИНЫ (МДК, ПМ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Код дисциплины:	МДК.02.01
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	МДК 01.01 Операционные системы
2.1.2	МДК 01.05 Эксплуатация компьютерных сетей
	МДК изучается во 2 семестре 2 курса и в 1,2 семестрах 3 курса
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (МДК, ПМ) необходимо как предшествующее:**
2.2.1	ПДП Преддипломная практика

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МДК, ПМ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ОК 01: Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
Знать: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности
Уметь: распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
ОК 02: Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
Знать: номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации
Уметь: определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска
ОК 03: Планировать и реализовывать собственное профессиональное и личностное развитие
Знать: содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования
Уметь: определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития
ОК 04: Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
Знать: психология коллектива; психология личности; основы проектной деятельности
Уметь: организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами
ОК 05: Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
Знать: особенности социального и культурного контекста; правила оформления документов.
Уметь: излагать свои мысли на государственном языке; оформлять документы.
ОК 06: Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
Знать: сущность гражданско-патриотической позиции; Общечеловеческие ценности; Правила поведения в ходе выполнения профессиональной деятельности
Уметь: описывать значимость своей профессии; Презентовать структуру профессиональной деятельности по

специальности
ОК 07: Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
Знать: правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения**.**
Уметь: соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности.
ОК 08: Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности
Знать: роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения.
Уметь: использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной специальности
ОК 09: Использовать информационные технологии в профессиональной деятельности
Знать: современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности.
Уметь: применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение
ОК 10: Пользоваться профессиональной документацией на государственном и иностранном языках
Знать: правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности
Уметь: понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы
ОК 11: Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере
Знать: методы планирования предпринимательской деятельности в профессиональной сфере.
Уметь: использовать полученные знания и опыт в организации предпринимательской деятельности в профессиональной сфере.
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации
Знать: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных
Уметь: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
Иметь практический опыт: установка, настройка программных средств защиты информации
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
Знать: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных
Уметь: устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
Иметь практический опыт: обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами; использование программных и программно-аппаратных средств для защиты информации в сети
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации
Знать: методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации
Уметь: диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;
Иметь практический опыт: тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа
Знать: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации
Уметь: применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения

криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись
Иметь практический опыт: решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств
Знать: особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации
Уметь: применять средства гарантированного уничтожения информации
Иметь практический опыт: учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак
Знать: типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа
Уметь: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак
Иметь практический опыт: работа с подсистемами регистрации событий; выявление событий и инцидентов безопасности в автоматизированной системе

В результате освоения дисциплины (МДК, ПМ) обучающийся должен

3.1	**Знать:**
	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности; номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации; содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования; психология коллектива; психология личности; основы проектной деятельности; особенности социального и культурного контекста; правила оформления документов; сущность гражданско-патриотической позиции; Общечеловеческие ценности; Правила поведения в ходе выполнения профессиональной деятельности; правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения; роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения; современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности; правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности; методы планирования предпринимательской деятельности в профессиональной сфере;.особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации; особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа
3.2	**Уметь:**

	распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника); определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска; определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития; организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами; излагать свои мысли на государственном языке; оформлять документы; описывать значимость своей профессии; Презентовать структуру профессиональной деятельности по специальности; соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности; использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной специальности; применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение; понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы; использовать полученные знания и опыт в организации предпринимательской деятельности в профессиональной сфере; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись; применять средства гарантированного уничтожения информации; осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак
3.3	**Иметь практический опыт:**
	установка, настройка программных средств защиты информации; обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами; использование программных и программно-аппаратных средств для защиты информации в сети; тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации; решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных; учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности; работа с подсистемами регистрации событий; выявление событий и инцидентов безопасности в автоматизированной системе

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МДК, ПМ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Примечание
	Раздел 1. Лекционные занятия					
1.1	Предмет и задачи программно-аппаратной защиты информации.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1	

1.2	Предмет и задачи программно-аппаратной защиты информации.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.3	Предмет и задачи программно-аппаратной защиты информации.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.4	Предмет и задачи программно-аппаратной защиты информации.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.5	Стандарты безопасности.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.6	Стандарты безопасности.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.7	Стандарты безопасности.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		

1.8	Стандарты безопасности.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.9	Защищенная автоматизированная система.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.10	Защищенная автоматизированная система.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.11	Защищенная автоматизированная система.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.12	Дестабилизирующее воздействие на объекты защиты.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.13	Дестабилизирующее воздействие на объекты защиты	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		

1.14	Дестабилизирующее воздействие на объекты защиты	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.15	Принципы программно-аппаратной защиты информации от несанкционированного доступа.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.16	Принципы программно-аппаратной защиты информации от несанкционированного доступа.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.17	Принципы программно-аппаратной защиты информации от несанкционированного доступа.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.18	Основы защиты автономных автоматизированных систем.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.19	Основы защиты автономных автоматизированных систем.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		

1.20	Защита программ от излучения.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.21	Вредоносное программное обеспечение.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.22	Вредоносное программное обеспечение.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.23	Вредоносное программное обеспечение.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.24	Защита программ и данных от несанкционированного копирования.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.25	Защита программ и данных от несанкционированного копирования.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		

1.26	Защита программ и данных от несанкционированного копирования.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.27	Защита информации на машинных носителях.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.28	Защита информации на машинных носителях.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.29	Защита информации на машинных носителях.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.30	Аппаратные средства идентификации и аутентификации пользователей.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.31	Аппаратные средства идентификации и аутентификации пользователей.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		

1.32	Системы обнаружения атак и вторжений.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.33	Системы обнаружения атак и вторжений.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.34	Системы обнаружения атак и вторжений.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.35	Основы построения защищенных сетей.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.36	Основы построения защищенных сетей.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.37	Основы построения защищенных сетей.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		

1.38	Средства организации VPN.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.39	Средства организации VPN.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.40	Средства организации VPN.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.41	Обеспечение безопасности межсетевого взаимодействия.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.42	Обеспечение безопасности межсетевого взаимодействия.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.43	Обеспечение безопасности межсетевого взаимодействия.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		

1.44	Защита информации в базах данных.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.45	Защита информации в базах данных.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.46	Защита информации в базах данных.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.47	Мониторинг систем защиты.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.48	Мониторинг систем защиты.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.49	Мониторинг систем защиты.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		

1.50	Изучение мер защиты информации в информационных системах.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.51	Изучение мер защиты информации в информационных системах.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.52	Изучение мер защиты информации в информационных системах.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.53	Изучение современных программно-аппаратных комплексов.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
1.54	Изучение современных программно-аппаратных комплексов.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
	Раздел 2. Практические занятия						
2.1	Учет, обработка, хранение и передача информации в АИС	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		

2.2	Учет, обработка, хранение и передача информации в АИС	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.3	Учет, обработка, хранение и передача информации в АИС	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.4	Учет, обработка, хранение и передача информации в АИС	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.5	Ограничение доступа на вход в систему.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5,	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.6	Ограничение доступа на вход в систему.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.7	Ограничение доступа на вход в систему.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		

2.8	Идентификация и аутентификация пользователей	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.9	Идентификация и аутентификация пользователей	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.10	Идентификация и аутентификация пользователей	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.11	Разграничение доступа.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.12	Разграничение доступа.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.13	Разграничение доступа.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		

2.14	Регистрация событий (аудит).	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.15	Регистрация событий (аудит).	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.16	Регистрация событий (аудит).	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.17	Контроль целостности данных	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.18	Контроль целостности данных	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.19	Контроль целостности данных	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		

2.20	Уничтожение остаточной информации.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.21	Уничтожение остаточной информации.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.22	Уничтожение остаточной информации.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.23	Управление политикой безопасности.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.24	Управление политикой безопасности.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.25	Шаблоны безопасности	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		

2.26	Шаблоны безопасности	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.27	Криптографическая защита.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.28	Криптографическая защита.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.29	Криптографическая защита.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.30	Криптографическая защита.	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.31	Обзор программ шифрования данных	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		

2.32	Обзор программ шифрования данных	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
2.33	Обзор программ шифрования данных	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
	Раздел 3. Лабораторные занятия						
3.1	Изучение механизмов защиты СУБД MS Access	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л3.1, Э1		
3.2	Изучение механизмов защиты СУБД MS Access	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л3.1, Э1		
3.3	Изучение механизмов защиты СУБД MS Access	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л3.1, Э1		
3.4	Изучение механизмов защиты СУБД MS Access	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л3.1, Э1		

3.5	Изучение штатных средств защиты СУБД MS SQLServer	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л3.1, Э1		
3.6	Изучение штатных средств защиты СУБД MS SQLServer	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л3.1, Э1		
3.7	Изучение штатных средств защиты СУБД MS SQLServer	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л3.1, Э1		
3.8	Изучение штатных средств защиты СУБД MS SQLServer	6/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л3.1, Э1		
	Раздел 4. Курсовое проектирование						
4.1	Выполнение курсового проекта по заданной теме	6/3	30	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
	Раздел 5. Контроль						
5.1	Другие формы промежуточной аттестации	4/2		ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5,	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		

5.2	Зачет	5/3		ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
5.3	Курсовой проект	6/3		ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Э1		
5.3	Экзамен	6/3	8	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л3.1, Э1		

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Размещен в приложении

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МДК, ПМ)

6.1. Рекомендуемая литература

6.1.1. Перечень основной литературы, необходимой для освоения дисциплины (МДК, ПМ)

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Язов Ю.К., Соловьев С.В.	Защита информации в информационных системах от несанкционированного доступа	Кварта, 2015
Л1.2.	Хорев П.Б.	Программно-аппаратная защита информации	Форум, 2012
Л1.3	Шаньгин В.Ф.	Защита компьютерной информации. Эффективные методы и средства	ДМК Пресс, 2008
Л1.4	Казарин О. В, Забабурин А. С.	Программно-аппаратные средства защиты информации. Защита программного обеспечения	Издательство Юрайт, 2019
Л1.5	Внуков А. А.	Защита информации	Издательство Юрайт, 2019

6.1.2. Перечень дополнительной литературы, необходимой для освоения дисциплины (МДК, ПМ)

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Каторин Ю.Ф., Разумовский А.В., Спивак А.И.	Защита информации техническими средствами	НИУ ИТМО, 2012
Л2.2	Мельников В.В.	Безопасность информации в автоматизированных системах	Финансы и статистика, 2003
Л2.3	Казарин О. В, Забабурин А. С.	Программно-аппаратные средства защиты информации. Защита программного обеспечения	Издательство Юрайт, 2019
Л2.4	Внуков А. А.	Защита информации	Издательство Юрайт, 2019

6.1.3. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (МДК, ПМ)

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Бирюков А.А.	Информационная безопасность : защита и нападение. Практическое пособие	ДМК Пресс, 2017

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (МДК, ПМ)		
Э1	Федеральная служба по техническому и экспортному контролю	www.fstec.ru

6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (МДК, ПМ), включая перечень программного обеспечения и информационных справочных систем (при необходимости)
6.3.1 Перечень программного обеспечения
-Win XP, 7
- DreamSpark Premium Electronic Software Delivery (3 years) Renewal 1203984220
- Kaspersky Endpoint Security 10 для Windows - 356¬160615-113525¬730¬94
- Права на ПО NetPolice School для Traffic Inspector Unlimited
- Права на ПО Traffic Inspector Anti-Virus powered by Kaspersky Special
-Traffic Inspector (Контракт 524 ДВГУПС от 15.07.2019)
Microsoft Windows Professional 10 Russian 1 License 5 шт,
базовый пакет для сертифицированной версии ОС Windows 8.1 Профессиональная/Pro для использования на 1 АРМ
Microsoft Office Professional Plus 2019 Russian OLP 1 License 18 шт,
программа контроля сертифицированной версии ОС Windows 8.1 Профессиональная 5 шт,
Microsoft Windows Server CAL 2019 Russian OLP 1 License User CAL 22 шт,
Базовый пакет для сертифицированной версии ОС Microsoft Windows Server Datacenter 2012 R2 для использования на 2 процессора 1 шт,
ОС Astra Linux Special Edition (Box версия с установочным комплектом) 5 шт. - Контракт № 1272401815819000324/157 ДВГУПС от 15.03.2019 г.
RedCheck Professional на 1 IP-адрес на 1 год 10 шт, КриптоПро CSP версии 4.0 5 шт,
Dallas Lock 8.0-C с модулями «Межсетевой экран» и «Система обнаружения и предотвращения вторжений». 5 шт,
Secret Net Studio 8 в редакции «Постоянная защита» (бессрочная) с модулями защиты от НСД, контроля устройств (СКН) и межсетевого экранирования (МЭ) 6 шт,
Антивирус Kaspersky Endpoint Security бизнеса – Расширенный Russian Edition. 1500-2499 Node 1 year Educational Renewal License 20шт. - Контракт № 1272401815819000584/290 ДВГУПС от 08.05.2019 г.
6.3.2 Перечень информационных справочных систем
1. Профессиональная база данных, информационно-справочная система Гарант - http://www.garant.ru
2. Профессиональная база данных, информационно-справочная система КонсультантПлюс - http://www.consultant.ru

7. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)		
Аудитория	Назначение	Оснащение
325	Учебная аудитория для проведения теоретических занятий (уроков), практических занятий, лабораторных работ, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, курсового проектирования. Компьютерный класс.	Комплект мебели. Технические средства обучения: персональный компьютер преподавателя, мультимедийное оборудование, 10 рабочих мест, оснащенных персональными компьютерами. - Win XP, 7 - DreamSpark Premium Electronic Software Delivery (3 years) Renewal 1203984220 - Kaspersky Endpoint Security 10 для Windows - 356¬160615-113525¬730¬94 - Права на ПО NetPolice School для Traffic Inspector Unlimited - Права на ПО Traffic Inspector Anti-Virus powered by Kaspersky Special -Traffic Inspector (Контракт 524 ДВГУПС от 15.07.2019)

320	Учебная аудитория для проведения теоретических занятий (уроков). Лекционная аудитория.	Комплект мебели, проектор, персональный компьютер, комплект презентаций. - Win XP, 7 - DreamSpark Premium Electronic Software Delivery (3 years) Renewal 1203984220 - Kaspersky Endpoint Security 10 для Windows - 356¬160615-113525¬730¬94 - Права на ПО NetPolice School для Traffic Inspector Unlimited - Права на ПО Traffic Inspector Anti-Virus powered by Kaspersky Special -Traffic Inspector (Контракт 524 ДВГУПС от 15.07.2019)
324	Учебная аудитория для проведения теоретических занятий (уроков), практических занятий, лабораторных работ, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория программных и программно-аппаратных средств защиты информации. Лаборатория "Защита информации от утечки за счет несанкционированного доступа в локальных вычислительных сетях".	Комплект учебной мебели, экран, автоматизированное рабочее место IZEC «Студент» в сборе 16 шт, Автоматизированное рабочее место IZEC «Преподаватель» в сборе 1 шт, автоматизированное рабочее место IZEC «Диспетчер АСУ ТП» в сборе 1 шт, сервер IZEC на платформе WOLF PASS 2U в сборе 1 шт, сервер IZEC на платформе SILVER PASS 1U в сборе 1 шт, Ноутбук HP 250 G6 15.6 1 шт, МФУ XEROX WC 6515DNI 1 шт, электронный идентификатор ruToken S 64 КБ 20 шт, электронный идентификатор JaCarta-2 PRO/ГОСТ 5 шт, средство доверенной загрузки Dallas Lock PCI-E Full Size 5 шт, средство доверенной загрузки "Соболь" версия 4 PCI-E 5 шт, рупор измерительный широкополосный П6-124 зав. № 150718305 в комплекте с диэлектрическим штативом, кабель КИ-18-5м-SMAM-SMAM, индуктор магнитный ИРМ-500М Зав. № 015, пробник напряжения Я6-122/1М Зав. № 024, токосъемник измерительный ТК-400М Зав. № 87, антенна измерительная дипольная активная АИ5-0 Зав. № 1742, мультимедийный проектор. Microsoft Windows Professional 10 Russian 1 License 5 шт, базовый пакет для сертифицированной версии ОС Windows 8.1 Профессиональная/Pro для использования на 1 АРМ 5шт, Microsoft Office Professional Plus 2019 Russian OLP 1 License 18 шт, программа контроля сертифицированной версии ОС Windows 8.1 Профессиональная 5 шт, Microsoft Windows Server CAL 2019 Russian OLP 1 License User CAL 22 шт, Базовый пакет для сертифицированной версии ОС Microsoft Windows Server Datacenter 2012 R2 для использования на 2 процессора 1 шт, ОС Astra Linux Special Edition (Box версия с установочным комплектом) 5 шт. - Контракт № 1272401815819000032 4/157 ДВГУПС от 15.03.2019 г. RedCheck Professional на 1 IP-адрес на 1 год 10 шт, КриптоПро CSP версии 4.0 5 шт, Dallas Lock 8.0-С с модулями «Межсетевой экран» и «Система обнаружения и предотвращения вторжений». 5 шт, Secret Net Studio 8 в редакции «Постоянная защита» (бессрочная) с модулями защиты от НСД, контроля устройств (СКН) и межсетевого экранирования (МЭ) 6 шт, Антивирус Kaspersky Endpoint Security бизнеса – Расширенный Russian Edition. 1500-2499 Node 1 year Educational Renewal License 20шт. - Контракт № 1272401815819000058 4/290 ДВГУПС от 08.05.2019 г.

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МДК, ПМ)

В процессе изучения дисциплины обучающиеся посещают лекции (уроки), практические и лабораторные занятия. На всех этапах обучения по МДК осуществляется контроль знаний.

Подготовка к лекциям (урокам), практическим и лабораторным занятиям включает изучение конспекта лекций, учебных пособий, основной и дополнительной литературы, законодательных и нормативных источников.

Лекция (урок). Работа на лекции является очень важным видом деятельности обучающихся для изучения дисциплины , т.к. лектор ориентирует обучающихся в учебном материале. Краткие записи лекций (конспектирование) помогает усвоить материал. Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины.

Практические и лабораторные занятия. Обучающиеся самостоятельно под руководством преподавателя выполняют задания по темам курса.

Курсовой проект. Цель курсового проекта – закрепление знаний и практических навыков, которые получены обучающимся при изучении дисциплины.. Обучающиеся выполняют курсовой проект под руководством преподавателя, выполненный проект сдается для проверки. Проект допускается к защите, и задача студента – защитить ее положительно. Неудовлетворительно выполненная работа подлежит переработке в соответствии с замечаниями преподавателя, содержащимися в рецензии. Защита курсового проекта - это специально организованная беседа преподавателя с обучающимся по разделам и рассчитанное на выяснение объема знаний обучающихся по определенному вопросу, теме, проблеме и т.п. Темы курсовых проектов приведены в приложении 1.

ОСНОВНЫЕ ПРАВИЛА ОФОРМЛЕНИЯ КУРСОВОГО ПРОЕКТА

Схемы, графики также нумеруются арабскими цифрами в пределах раздела и обозначаются термином «Рисунок», являющимся первым словом в подрисуночной подписи, которая приводится ниже иллюстрации шрифтом на 2 пт меньше основного.

Приводимые в тексте цитаты должны соответствовать оригиналу и иметь на него ссылку, которую оформляют в квадратных скобках номером источника, согласно списку использованной литературы. Затем ставится запятая и номер страницы (например, [5, с. 124]. Также оформляется ссылка на реферируемый источник, только без указания страниц.

Список используемых источников приводится в следующей последовательности: Законы РФ, Указы Президента, Постановления Правительства, Положения, другие нормативные акты, далее размещаются все остальные источники в алфавитном порядке. Текст отчета оформляется на листах стандартного формата (297×210), заполненных с одной стороны, размер полей: левое – 30 мм, правое – 10 мм, верхнее и нижнее – 20 мм; шрифт Times New Roman 14, обычный; выравнивание по ширине; абзацный отступ 15 мм; межстрочный интервал 1,5; автоматический перенос слов. Первым листом текста является титульный лист (номер не ставится), вторым – содержание с указанием номеров страниц частей работы. Страницы нумеруются арабскими цифрами, которые располагаются в центре страницы.

Разделы и подразделы должны иметь нумерацию и обозначаются арабскими цифрами. Номера подразделов устанавливаются в рамках раздела и имеют двухзначный номер, цифры которого разделяются точкой (например, первый подраздел второго раздела будет иметь номер 2.1).

Структурные части проекта (содержание, введение, заключение, список использованных источников) не нумеруются, а их название размещается по центру страницы. Приложения к отчету, упоминание о них с указанием наименования отражается в содержании после списка использованных источников, они обозначаются заглавными буквами (А, Б и т.д., кроме букв Е, З, Й, О, Ч, Ь Ы, Ъ). Например: «Приложение А. Системы охраны участка».

Каждый раздел проекта необходимо оформлять с новой страницы, перед текстом с абзацного отступа пишется название раздела, затем первого подраздела обычным шрифтом. Эти названия не подчеркиваются, полужирный шрифт и курсив не используются. Размещение подразделов следует друг за другом.

Таблицы, рисунки приводятся по тексту, после первого упоминания о них, таблицы нумеруются арабскими цифрами в пределах раздела и располагаются с абзаца (слева), затем в одну строку после слова «Таблица» и знака «-» пишется ее заголовок. Размер текста таблицы – 12 кегль.

Допускается перенос таблицы на следующую страницу, но при этом ее «шапка» без текста при переносе не должна оставаться на предыдущей странице. На новой странице над продолжающейся таблицей пишется нумерационный заголовок «Продолжение таблицы 3.1», если она не закончена, или «Окончание таблицы 3.1», если закончена, с выравниванием по левому краю. Название таблицы не повторяется, но повторяется шапка таблицы (заголовки и подзаголовки столбцов).

Схемы, графики также нумеруются арабскими цифрами в пределах раздела и обозначаются термином «Рисунок», являющимся первым словом в подрисуночной подписи, которая приводится ниже иллюстрации шрифтом на 2 пт меньше основного.

Приводимые в тексте цитаты должны соответствовать оригиналу и иметь на него ссылку, которую оформляют в квадратных скобках номером источника, согласно списку использованной литературы. Затем ставится запятая и номер страницы (например, [5, с. 124]. Также оформляется ссылка на реферируемый источник, только без указания страниц.

Список используемых источников приводится в следующей последовательности: Законы РФ, Указы Президента, Постановления Правительства, другие нормативные акты, далее размещаются все остальные источники в алфавитном порядке

МДК.02.02 «*Криптографические средства защиты информации*»

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МДК, ПМ)	
1.1	Математические основы криптографии. Методы криптографического защиты информации. Классификация основных методов криптографической защиты. Гаммирование. Криптоанализ. Криптографическая стойкость. Перспективные направления криптоанализа, квантовый криптоанализ. Поточные шифры и генераторы псевдослучайных чисел. Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS. Кодирование информации. Компьютеризация шифрования. Компьютеризация шифрования. Аппаратное и программное шифрование. Симметричные системы шифрования. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4. Асимметричные системы шифрования. Аутентификация данных. Электронная подпись. Алгоритмы обмена ключей и протоколы аутентификации. Криптозащита информации в сетях передачи данных. Защита информации в электронных платежных системах. Компьютерная стеганография.

2. МЕСТО ДИСЦИПЛИНЫ (МДК, ПМ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Код дисциплины:	МДК.02.02
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	МДК 01.01 Операционные системы
2.1.2	МДК 01.05 Эксплуатация компьютерных сетей
	МДК изучается в 2 семестре 2 курса и 1 семестре 3 курса
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (МДК, ПМ) необходимо как предшествующее:**
2.2.1	МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации
2.2.2	ПП 02.01. Производственная практика
2.2.2	ПДП Преддипломная практика

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МДК, ПМ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ОК 01: Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
Знать: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности
Уметь: распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
ОК 02: Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
Знать: номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации
Уметь: определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска
ОК 03: Планировать и реализовывать собственное профессиональное и личностное развитие
Знать: содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования
Уметь: определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития
ОК 04: Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
Знать: психология коллектива; психология личности; основы проектной деятельности
Уметь: организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами
ОК 05: Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
Знать: особенности социального и культурного контекста; правила оформления документов.
Уметь: излагать свои мысли на государственном языке; оформлять документы.
ОК 06: Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
Знать: сущность гражданско-патриотической позиции; Общечеловеческие ценности; Правила поведения в ходе выполнения профессиональной деятельности

Уметь: описывать значимость своей профессии; Презентовать структуру профессиональной деятельности по специальности
ОК 07: Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
Знать: правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения**.**
Уметь: соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности.
ОК 08: Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности
Знать: роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения.
Уметь: использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной специальности
ОК 09: Использовать информационные технологии в профессиональной деятельности
Знать: современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности.
Уметь: применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение
ОК 10: Пользоваться профессиональной документацией на государственном и иностранном языках
Знать: правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности
Уметь: понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы
ОК 11: Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере
Знать: методы планирования предпринимательской деятельности в профессиональной сфере.
Уметь: использовать полученные знания и опыт в организации предпринимательской деятельности в профессиональной сфере.
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа
Знать: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации
Уметь: применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись
Иметь практический опыт: решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных

В результате освоения дисциплины (МДК, ПМ) обучающийся должен

3.1	**Знать:**

	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности; номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации; содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования; психология коллектива; психология личности; основы проектной деятельности; особенности социального и культурного контекста; правила оформления документов; сущность гражданско-патриотической позиции; Общечеловеческие ценности; Правила поведения в ходе выполнения профессиональной деятельности; правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения; роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения; современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности; правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности; методы планирования предпринимательской деятельности в профессиональной сфере; особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации
3.2	**Уметь:**
	распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника); определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска; определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития; организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами; излагать свои мысли на государственном языке; оформлять документы; описывать значимость своей профессии; Презентовать структуру профессиональной деятельности по специальности; соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности; использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной специальности; применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение; понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы; использовать полученные знания и опыт в организации предпринимательской деятельности в профессиональной сфере; применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись
3.3	**Иметь практический опыт:** решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МДК, ПМ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература		Примечание
	Раздел 1. Лекционные занятия						
1.1	Математические основы криптографии.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.2	Математические основы криптографии.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.3	Методы криптографического защиты информации.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.4	Методы криптографического защиты информации.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.5	Классификация основных методов криптографической защиты.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.6	Классификация основных методов криптографической защиты.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.7	Гаммирование. Криптоанализ.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.8	Криптографическая стойкость.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.9	Перспективные направления криптоанализа.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		

1.10	Квантовый криптоанализ.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.11	Поточные шифры и генераторы псевдослучайных чисел.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.12	Поточные шифры и генераторы псевдослучайных чисел.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.13	Методы получения псевдослучайных последовательностей.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.14	ЛКГ, метод Фибоначчи, метод BBS.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.15	Кодирование информации.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.16	Компьютеризация шифрования.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.17	Компьютеризация шифрования.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.18	Аппаратное и программное шифрование.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.19	Симметричные системы шифрования.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		

1.20	Симметричные системы шифрования	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.21	Симметричные системы шифрования	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.22	Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.23	Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.24	Асимметричные системы шифрования.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.25	Асимметричные системы шифрования.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.26	Аутентификация данных.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.27	Электронная подпись.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.28	Алгоритмы обмена ключей и протоколы аутентификации.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.29	Алгоритмы обмена ключей и протоколы аутентификации.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		

1.30	Криптозащита информации в сетях передачи данных.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.31	Криптозащита информации в сетях передачи данных.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.32	Защита информации в электронных платежных системах.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.33	Защита информации в электронных платежных системах.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.34	Компьютерная стеганография.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
1.35	Компьютерная стеганография.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
	Раздел 2. Практические занятия						
2.1	Применение метода гаммирования	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
2.2	Применение метода гаммирования	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
2.3	Применение метода гаммирования	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		

2.4	Криптоанализ классических шифров	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
2.5	Криптоанализ классических шифров	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
2.6	Криптоанализ классических шифров	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
2.7	Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
2.8	Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
2.9	Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.	4/2	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
2.10	Применение различных асимметричных алгоритмов.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
2.11	Применение различных асимметричных алгоритмов.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
2.12	Применение различных асимметричных алгоритмов.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
2.13	Применение различных функций хеширования.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		

2.14	Анализ особенностей хешей	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
2.15	Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
2.16	Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
2.17	Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	5/3	1	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
	Раздел 3. Лабораторные занятия						
3.1	Применение аутентификации по одноразовым паролям.	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
3.2	Реализация алгоритмов создания одноразовых паролей	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
3.3	Реализация простейших стенографических алгоритмов	5/3	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
	Раздел 4. Контроль						
4.1	Дифференцированный зачет	4/2		ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		
4.2	Экзамен	5/3	8	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л3.1, Л3.2, Л3.3, Э1, Э2, Э3, Э4, Э5, Э6		

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Размещен в приложении

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МДК, ПМ)

6.1. Рекомендуемая литература

6.1.1. Перечень основной литературы, необходимой для освоения дисциплины (МДК, ПМ)

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Романьков В. А.	Алгебраическая криптография	Омск: Омский государственный университет, 2013, http://biblioclub.ru/index.php?page=book&id=238045
Л1.2	Фороузан Б. А.	Математика криптографии и теория шифрования	Москва: Национальный Открытый Университет «ИНТУИТ», 2016, http://biblioclub.ru/index.php?page=book&id=428998

6.1.2. Перечень дополнительной литературы, необходимой для освоения дисциплины (МДК, ПМ)

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Лапонина О. Р.	Криптографические основы безопасности	Москва: Национальный Открытый Университет «ИНТУИТ», 2016, http://biblioclub.ru/index.php?page=book&id=429092
Л2.2	Молдовян А.А., Молдовян Н.А.	Криптография: учебник	Санкт-Петербург: Лань, 2001,

6.1.3. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (МДК, ПМ)

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Анисимов В.В.	Криптография: Метод. указания по выполнению лаб. работ по дисц. "Информ. безопасность и защита	Хабаровск: Изд-во ДВГУПС, 2004
Л3.2	Долгов В.А., Анисимов В.В.	Криптографические методы защиты информации: учеб. пособие	Хабаровск: Изд-во ДВГУПС, 2008
Л3.3	Коломийцева С.В.	Введение в эллиптическую криптографию: метод. пособие по выполнению лабораторной работы	Хабаровск: Изд-во ДВГУПС, 2012

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (МДК, ПМ)

Э1	Электронно-библиотечная система «Университетская библиотека ONLINE»	biblioclub.ru
Э2	Галатенко, В.А. Основы информационной безопасности.	www.intuit.ru
Э3	Басалова, Г.В. Основы криптографии.	www.intuit.ru
Э4	Галатенко, В.А. Информационная безопасность: основные стандарты и	www.intuit.ru
Э5	Учебная и научная деятельность Анисмова В.В.	sites.google.com/site/anisimovk hv
Э6	ЦИК РФ	cikrf.ru

6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (МДК, ПМ), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

6.3.1 Перечень программного обеспечения

Win XP, 7
- DreamSpark Premium Electronic Software Delivery (3 years) Renewal 1203984220
- Kaspersky Endpoint Security 10 для Windows - 356¬160615-113525¬730¬94
- Права на ПО NetPolice School для Traffic Inspector Unlimited
- Права на ПО Traffic Inspector Anti-Virus powered by Kaspersky Special
-Traffic Inspector (Контракт 524 ДВГУПС от 15.07.2019)
Microsoft Windows Professional 10 Russian 1 License 5 шт,
Базовый пакет для сертифицированной версии ОС Windows 8.1 Профессиональная/Pro для использования на 1
Microsoft Office Professional Plus 2019 Russian OLP 1 License 18 шт,
программа контроля сертифицированной версии ОС Windows 8.1 Профессиональная 5 шт,
Microsoft Windows Server CAL 2019 Russian OLP 1 License User CAL 22 шт,
Базовый пакет для сертифицированной версии ОС Microsoft Windows Server Datacenter 2012 R2 для использования на 2 процессора 1 шт,

ОС Astra Linux Special Edition (Box версия с установочным комплектом) 5 шт. - Контракт № 1272401815819000324/157 ДВГУПС от 15.03.2019 г.
RedCheck Professional на 1 IP-адрес на 1 год 10 шт, КриптоПро CSP версии 4.0 5 шт,
Dallas Lock 8.0-C с модулями «Межсетевой экран» и «Система обнаружения и предотвращения вторжений». 5 шт,
Secret Net Studio 8 в редакции «Постоянная защита» (бессрочная) с модулями защиты от НСД, контроля устройств (СКН) и межсетевого экранирования (МЭ) 6 шт,
Антивирус Kaspersky Endpoint Security бизнеса – Расширенный Russian Edition. 1500-2499 Node 1 year Educational Renewal License 20шт. - Контракт № 1272401815819000584/290 ДВГУПС от 08.05.2019 г.
6.3.2 Перечень информационных справочных систем
1. Профессиональная база данных, информационно-справочная система Гарант - http://www.garant.ru
2. Профессиональная база данных, информационно-справочная система КонсультантПлюс - http://www.consultant.ru

7. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Аудитория	Назначение	Оснащение
325	Учебная аудитория для проведения теоретических занятий (уроков), практических занятий, лабораторных работ, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, курсового проектирования. Компьютерный класс.	Комплект мебели. Технические средства обучения: персональный компьютер преподавателя, мультимедийное оборудование, 10 рабочих мест, оснащенных персональными компьютерами. - Win XP, 7 - DreamSpark Premium Electronic Software Delivery (3 years) Renewal 1203984220 - Kaspersky Endpoint Security 10 для Windows - 356¬160615-113525¬730¬94 - Права на ПО NetPolice School для Traffic Inspector Unlimited - Права на ПО Traffic Inspector Anti-Virus powered by Kaspersky Special -Traffic Inspector (Контракт 524 ДВГУПС от 15.07.2019)

324	Учебная аудитория для проведения теоретических занятий (уроков), практических занятий, лабораторных работ, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория программных и программно-аппаратных средств защиты информации. Лаборатория "Защита информации от утечки за счет несанкционированного доступа в локальных вычислительных сетях".	Комплект учебной мебели, экран, автоматизированное рабочее место IZEC «Студент» в сборе 16 шт, Автоматизированное рабочее место IZEC «Преподаватель» в сборе 1 шт, автоматизированное рабочее место IZEC «Диспетчер АСУ ТП» в сборе 1 шт, сервер IZEC на платформе WOLF PASS 2U в сборе 1 шт, сервер IZEC на платформе SILVER PASS 1U в сборе 1 шт, Ноутбук HP 250 G6 15.6 1 шт, МФУ XEROX WC 6515DNI 1 шт, электронный идентификатор ruToken S 64 КБ 20 шт, электронный идентификатор JaCarta-2 PRO/ГОСТ 5 шт, средство доверенной загрузки Dallas Lock PCI-E Full Size 5 шт, средство доверенной загрузки "Соболь" версия 4 PCI-E 5 шт, рупор измерительный широкополосный П6-124 зав. № 150718305 в комплекте с диэлектрическим штативом, кабель КИ-18-5м-SMAM-SMAM, индуктор магнитный ИРМ-500М Зав. № 015, пробник напряжения Я6-122/1М Зав. № 024, токосъемник измерительный ТК-400М Зав. № 87, антенна измерительная дипольная активная АИ5-0 Зав. № 1742, мультимедийный проектор. Microsoft Windows Professional 10 Russian 1 License 5 шт, базовый пакет для сертифицированной версии ОС Windows 8.1 Профессиональная/Pro для использования на 1 АРМ 5шт, Microsoft Office Professional Plus 2019 Russian OLP 1 License 18 шт, программа контроля сертифицированной версии ОС Windows 8.1 Профессиональная 5 шт, Microsoft Windows Server CAL 2019 Russian OLP 1 License User CAL 22 шт, Базовый пакет для сертифицированной версии ОС Microsoft Windows Server Datacenter 2012 R2 для использования на 2 процессора 1 шт, ОС Astra Linux Special Edition (Box версия с установочным комплектом) 5 шт. - Контракт № 12724018158190000324/157 ДВГУПС от 15.03.2019 г. RedCheck Professional на 1 IP-адрес на 1 год 10 шт, КриптоПро CSP версии 4.0 5 шт, Dallas Lock 8.0-C с модулями «Межсетевой экран» и «Система обнаружения и предотвращения вторжений». 5 шт, Secret Net Studio 8 в редакции «Постоянная защита» (бессрочная) с модулями защиты от НСД, контроля устройств (СКН) и межсетевого экранирования (МЭ) 6 шт, Антивирус Kaspersky Endpoint Security бизнеса – Расширенный Russian Edition. 1500-2499 Node 1 year Educational Renewal License 20шт. - Контракт № 12724018158190000584/290 ДВГУПС от 08.05.2019 г.

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МДК, ПМ)

В процессе изучения дисциплины обучающиеся посещают лекции (уроки), практические и лабораторные занятия. На всех этапах обучения по МДК осуществляется контроль знаний.

Лекция (урок). Работа на лекции является очень важным видом деятельности обучающихся для изучения дисциплины , т.к. лектор ориентирует обучающихся в учебном материале. Краткие записи лекций (конспектирование) помогает усвоить материал. Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины.

Практические и лабораторные занятия. Обучающиеся самостоятельно под руководством преподавателя выполняют задания по темам курса.

Приложение 1

Оценочные материалы при формировании рабочей программы
ПМ.02 «Защита информации а автоматизированных системах программными и программно-аппаратными средствами»

МДК.02.01 «Программные и программно-аппаратные средства защиты информации»

1. Описание показателей, критериев и шкал оценивания компетенций.

Показатели и критерии оценивания компетенций ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК6, ОК7, ОК8, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6

Объект оценки	Уровни сформированности компетенций	Критерий оценивания результатов обучения
Обучающийся	Низкий уровень Пороговый уровень Повышенный уровень Высокий уровень	Уровень результатов обучения **не ниже порогового**

1.2. Шкалы оценивания компетенций ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК6, ОК7, ОК8, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6 при сдаче других форм промежуточной аттестации (устного опроса) и экзамена

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания
		Устный опрос (Экзамен)
Низкий уровень	Обучающийся: -обнаружил пробелы в знаниях основного учебно-программного материала; -допустил принципиальные ошибки в выполнении заданий, предусмотренных программой; -не может продолжить обучение или приступить к профессиональной деятельности по окончании программы без дополнительных занятий по соответствующей дисциплине.	Неудовлетворительно
Пороговый уровень	Обучающийся: -обнаружил знание основного учебно-программного материала в объёме, необходимом для дальнейшей учебной и предстоящей профессиональной деятельности; -справляется с выполнением заданий, предусмотренных программой; -знаком с основной литературой, рекомендованной рабочей программой дисциплины; -допустил неточности в ответе на вопросы и при выполнении заданий по учебно-программному материалу, но обладает необходимыми знаниями для их устранения под руководством преподавателя.	Удовлетворительно
Повышенный уровень	Обучающийся: - обнаружил полное знание учебно-программного материала; -успешно выполнил задания, предусмотренные программой; -усвоил основную литературу, рекомендованную рабочей программой дисциплины; -показал систематический характер знаний учебно-программного материала; -способен к самостоятельному пополнению знаний по учебно-программному материалу и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.	Хорошо
Высокий уровень	Обучающийся: -обнаружил всесторонние, систематические и глубокие знания учебно-программного материала; -умеет свободно выполнять задания, предусмотренные программой; -ознакомился с дополнительной литературой; -усвоил взаимосвязь основных понятий дисциплин и их значение для приобретения профессии; -проявил творческие способности в понимании учебно-программного материала.	Отлично

1.3. Шкалы оценивания компетенций ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК6, ОК7, ОК8, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6 при сдаче зачета.

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания
Пороговый уровень	Обучающийся: - обнаружил на зачете всесторонние, систематические и глубокие знания учебно-программного материала; - допустил небольшие упущения в ответах на вопросы, существенным образом не снижающие их качество; - допустил существенное упущение в ответе на один из вопросов, которое за тем было устранено студентом с помощью уточняющих вопросов; - допустил существенное упущение в ответах на вопросы, часть из которых была устранена студентом с помощью уточняющих вопросов	Зачтено
Низкий уровень	Обучающийся: - допустил существенные упущения при ответах на все вопросы преподавателя; - обнаружил пробелы более чем 50% в знаниях основного учебно-программного материала	Не зачтено

1.4. Шкалы оценивания компетенций ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК6, ОК7, ОК8, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6 при защите курсового проекта

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания
Низкий уровень	Содержание работы не удовлетворяет требованиям, предъявляемым к КП; на защите КП обучающийся не смог обосновать результаты проведенных расчетов (исследований); цель КП не достигнута; структура работы нарушает требования нормативных документов; выводы отсутствуют или не отражают теоретические положения, обсуждаемые в работе; в работе много орфографических ошибок, опечаток и других технических недостатков; язык не соответствует нормам научного стиля речи.	Неудовлетворительно
Пороговый уровень	Содержание работы удовлетворяет требованиям, предъявляемым к КП; на защите КП обучающийся не смог обосновать все результаты проведенных расчетов (исследований); задачи КП решены не в полном объеме, цель не достигнута; структура работы отвечает требованиям нормативных документов; выводы присутствуют, но не полностью отражают теоретические положения, обсуждаемые в работе; в работе присутствуют орфографические ошибки, опечатки; язык соответствует нормам научного стиля речи; при защите КП обучающийся излагает материал неполно и допускает неточности в определении понятий или формулировке правил; затрудняется или отвечает не правильно на поставленный вопрос	Удовлетворительно
Повышенный уровень	Содержание работы удовлетворяет требованиям, предъявляемым к КП; на защите КП обучающийся смог обосновать все результаты проведенных расчетов (исследований); задачи КП решены в полном объеме, цель достигнута; структура работы отвечает требованиям нормативных документов; выводы присутствуют, но не полностью отражают теоретические положения, обсуждаемые в работе; в работе практически отсутствуют орфографические ошибки, опечатки; язык соответствует нормам научного стиля речи; при защите КП полно обучающийся излагает материал, дает правильное определение основных понятий; затрудняется или отвечает не правильно на некоторые вопросы	Хорошо
Высокий	Содержание работы удовлетворяет требованиям, предъявляемым к КП; на защите КП обучающийся смог обосновать все результаты проведенных расчетов (исследований); задачи КП решены в полном объеме, цель достигнута; структура работы отвечает требованиям нормативных документов; выводы присутствуют и полностью отражают теоретические положения, обсуждаемые в работе; в работе отсутствуют орфографические ошибки, опечатки; язык соответствует нормам научного стиля речи; при защите КП обучающийся полно излагает материал, дает правильное определение основных понятий; четко и грамотно отвечает на вопросы	Отлично

1.5. Описание шкал оценивания

Компетенции обучающегося оценивается следующим образом:

Планируемый уровень результатов освоения	Содержание шкалы оценивания достигнутого уровня результата обучения			
	Неудовлетворительно (Не зачтено)	Удовлетворительно (Зачтено)	Хорошо (Зачтено)	Отлично (Зачтено)
Знать	Неспособность обучающегося самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся способен самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся демонстрирует способность к самостоятельному применению знаний при решении заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует способность к самостоятельному применению знаний в выборе способа решения неизвестных или нестандартных заданий и при консультативной поддержке в части междисциплинарных связей.
Уметь	Отсутствие у обучающегося самостоятельности в применении умений по использованию методов освоения учебной дисциплины.	Обучающийся демонстрирует самостоятельность в применении умений решения учебных заданий в полном соответствии с образцом, данным преподавателем.	Обучающийся продемонстрирует самостоятельное применение умений решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение умений решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.
Иметь практический опыт	Неспособность самостоятельно проявить навык решения поставленной задачи по стандартному образцу повторно.	Обучающийся демонстрирует самостоятельность в применении навыка по заданиям, решение которых было показано преподавателем.	Обучающийся демонстрирует самостоятельное применение навыка решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение навыка решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.

2. Перечень вопросов к другим формам промежуточной аттестации (устному опросу), зачету, защите курсового проекта, экзамену.

2.1 Примерный перечень вопросов к другим формам промежуточной аттестации (устному опросу).
Компетенции ОК 01, ОК 02, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6

1. Цели и средства защиты информации. Типичный набор функциональных подсистем.
2. Основные принципы организации защиты информации от НСД и обеспечения ее конфиденциальности.
3. Понятие Защищенной системы обработки информации. Стандарты информационной безопасности и их роль.
4. Понятие угрозы безопасности компьютерной системы. Методы «взлома» компьютерных систем.
5. Защита компьютерной системы от «взлома». Программные закладки.
6. Методы уничтожения информации, хранимой на энергонезависимых носителях. Уровни степеней надежности.
7. Защита программного обеспечения. Превентивные меры защиты.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6

8. Защита программного обеспечения. Средства активной защиты.
9. Защита программного обеспечения. Средства пассивной защиты.
10. Технология защиты информации на основе: электронных ключей, смарткарт, персональных идентификаторов.
11. Принципы и методы создания защищенной операционной системы.

12. Защита ресурсов ПЭВМ на аппаратном уровне.
13 Понятие замкнутой программной среды. Методология реализации. Мониторы безопасности объектов и субъектов.
14. Формирование и поддержка изолированной программной среды.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3
15. Программно-аппаратный комплекс СЗИ от НСД «АККОРД». Назначение, основные возможности.
16. Система защиты конфиденциальной информации «STRONGDISK». Назначение, основные возможности.
17. Система защиты корпоративной информации «SECRET DISK». Назначение, основные возможности.
18. Средство криптографической защиты информации «Верба». Назначение, основные возможности.
19. Средство криптографической защиты информации, криптопровайдер, «КриптоПРО». Назначение, основные возможности.
20. Комплексная система защиты информации «ПАНЦИРЬ». Назначение, основные возможности.
21. Система защиты информации от несанкционированного доступа «Аура». Назначение, основные возможности.

2.2 Примерный перечень вопросов к зачету.
Компетенции ОК 01, ОК 02, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6
1. Цели и средства защиты информации. Типичный набор функциональных подсистем.
2. Основные принципы организации защиты информации от НСД и обеспечения ее конфиденциальности.
3. Понятие Защищенной системы обработки информации. Стандарты информационной безопасности и их роль.
4. Понятие угрозы безопасности компьютерной системы. Методы «взлома» компьютерных систем.
5. Защита компьютерной системы от «взлома». Программные закладки.
6. Методы уничтожения информации, хранимой на энергонезависимых носителях. Уровни степеней надежности.
7. Защита программного обеспечения. Превентивные меры защиты.
8. Защита программного обеспечения. Средства собственной защиты.
9. Защита программного обеспечения. Средства защиты в составе вычислительной системы.
10. Защита программного обеспечения. Средства защиты с запросом информации.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6
11. Защита программного обеспечения. Средства активной защиты.
12. Защита программного обеспечения. Средства пассивной защиты.
13. Технология защиты информации на основе: электронных ключей, смарткарт, персональных идентификаторов.
14. Принципы и методы создания защищенной операционной системы.
15. Защита ресурсов ПЭВМ на аппаратном уровне.
16. Понятие замкнутой программной среды. Методология реализации. Мониторы безопасности объектов и субъектов.
17. Формирование и поддержка изолированной программной среды.
18. Политика безопасности защищенных компьютерных систем. Описательные категории.
19. Безопасное взаимодействие в КС.
20. Контроль и управление доступом.
21. Управление криптографическими ключами и хранение ключевой информации.
22. Концепция иерархии ключей. Распределение ключей.
23. Распределение ключей с участием центра распределения ключей. Протокол Kerberos.
24. СЗИ от НСД «Страж». Назначение, основные возможности.
25. СЗИ от НСД «DALLAS LOCK». Назначение, основные возможности.
26. СЗИ «SECRET NET». Назначение, основные возможности.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3
27. Программно-аппаратный комплекс СЗИ от НСД «АККОРД». Назначение, основные возможности.
28. Система защиты конфиденциальной информации «STRONGDISK». Назначение, основные возможности.
29. Система защиты корпоративной информации «SECRET DISK». Назначение, основные возможности.
30. Средство криптографической защиты информации «Верба». Назначение, основные возможности.
31. Средство криптографической защиты информации, криптопровайдер, «КриптоПРО». Назначение, основные возможности.
32. Комплексная система защиты информации «ПАНЦИРЬ». Назначение, основные возможности.
33. Система защиты информации от несанкционированного доступа «Аура». Назначение, основные возможности.
34. Аппаратно-программный модуль доверенной загрузки «КРИПТОНЗАМОК». Назначение, основные возможности.
35. СЗИ НСД «Блокпост». Назначение, основные возможности.
36. Система защиты информации «ЩИТ-РЖД». Назначение, основные возможности.
37. Система защиты информации ViPNet DISCguise. Назначение, основные возможности.
38. Система защиты информации ViPNet SafeDisk. Назначение, основные возможности.
39. Электронный замок «Соболь».
40. Назначение, основные возможности электронного замка «Соболь»

2.3 Темы курсовых проектов. Примерный перечень вопросов к защите курсового проекта.

2.3.1 Темы курсовых проектов.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК6, ОК7, ОК8, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6

1. Анализ аппаратных средств защиты ПК
2. Разработка ПС на основе асимметричного шифрования для защиты ОС.
3. Разработка ПС для защиты ОС с помощью цветовой схемы.
4. Разработка программно-аппаратного комплекса для защиты ОС.
5. Разработка электронного ключа для защиты от несанкционированного доступа к ПК
6. Разработка ПС для защиты от спама
7. Разработка ПС для защиты ПК от несанкционированного сканирования портов.
8. Анализ существующих методов защиты ОС
9. Разработка ПС для защиты от фишинговых атак
10. Разработка ПС для защиты ПК от несанкционированного сканирования портов.
11. Разработка электронного ключа для доступа к ПК
12. Разработка межсетевого экрана
13. Создание системы защиты локальной сети от несанкционированного доступа
14. Разработка системы управления сайтом с дополнительной аутентификацией пользователя
15. Разработка ПС для аутентификации пользователя с помощью графического изображения.
16. Разработка аппаратно-программного комплекса защиты ПК
17. Анализ существующих ПС по защите локальных сетей от внешних атак
18. Анализ существующих методов защиты ОС Linux
19. Разработка программного средства защиты ОС Linux
20. Разработка комплексной системы защиты серверной ОС

2.3.2 Примерный перечень вопросов к защите курсового проекта.

Компетенции ОК 01, ОК 02, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6

1. Цели и средства защиты информации. Типичный набор функциональных подсистем.
2. Основные принципы организации защиты информации от НСД и обеспечения ее конфиденциальности.
3. Понятие Защищенной системы обработки информации. Стандарты информационной безопасности и их роль.
4. Понятие угрозы безопасности компьютерной системы. Методы «взлома» компьютерных систем.
5. Защита компьютерной системы от «взлома». Программные закладки.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6

6. Методы уничтожения информации, хранимой на энергонезависимых носителях. Уровни степеней надежности.
7. Защита программного обеспечения. Превентивные меры защиты.
8. Защита программного обеспечения. Средства собственной защиты.
9. Защита программного обеспечения. Средства защиты в составе вычислительной системы.
10. Защита программного обеспечения. Средства защиты с запросом информации.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3

11. Защита программного обеспечения. Средства активной защиты.
12. Защита программного обеспечения. Средства пассивной защиты.
13. Технология защиты информации на основе: электронных ключей, смарткарт, персональных идентификаторов.
14. Принципы и методы создания защищенной операционной системы.
15. Защита ресурсов ПЭВМ на аппаратном уровне.

2.4 Примерный перечень вопросов к экзамену. Образец экзаменационного билета.

2.4.1 Примерный перечень вопросов к экзамену.

Компетенции ОК 01, ОК 02, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6

1) Семейство ОС Windows.
2) Этапы установки Windows.
3) Аппаратные требования Windows.
4) RAID. Аппаратный и программный. Типы.
5) RAID в Windows.
6) Работа с дисками в Windows.
7) Источники резервного питания
8) Резервное копирование данных.
9) Аппаратные устройства для разграничения доступа в сети.
10) Служба каталогов Windows.
11) Домен, дерево, лес в службе каталогов Windows.
12) Выбор аппаратных компонентов для организации серверных центров.
13) Служба каталогов Active Directory.
14) Установка и настройка AD.
15) Управление пользователями с помощью AD.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6

16) Группы в AD. Типы групп.
17) Разграничение доступа к ресурсам.
18) Система безопасности Windows.
19) Политика безопасности, наследование политики безопасности
20) Протокол безопасности Kerberos.
21) Firewall: назначение, принцип работы.
22) Microsoft ISA Server: особенности установки и настройки.
23) Виды адресаций в TCP/IP сетях
24) IP адрес: назначение, структура, применение
25) DNS имя: назначение, структура, применение
26) Семиуровневая модель OSI.
27) Характеристика стэка протоколов TCP/IP.
28) Виды адресации в IP сетях.
29) Протокол IP: назначение, структура заголовка, принципы работы
30) Протокол TCP: назначение, структура заголовка, основные режимы работы
31) Маршрутизация. Таблицы маршрутизации

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3
32) Службы Windows для мониторинга и оптимизации.
33) Мониторинг и оптимизация производительности дисков.
34) Работа с дисковыми квотами.
35) Сжатие и шифрование данных средствами ОС.
36) Консоль "Производительность": назначение, состав.
37) Оснастка "Системный монитор"
38) Оснастка "Журналы"
39) Утилита "Диспетчер задач": назначение, функции.
40) Описание протоколов VPN
41) Компоненты VipNet
42) Secret Net назначение и функции
43) Основные особенности использования Secret Net
44) Сравнительная характеристика Proxy и Nat серверов
45) Протокол безопасности IpSec
46) Программно-аппаратный комплекс "Соболь": назначение, установка, настройка

2.4.2. Образец экзаменационного билета по МДК 02.01

<table>
<tr><td colspan="3">Дальневосточный государственный университет путей сообщения</td></tr>
<tr><td>ПЦК
«Информационная безопасность автоматизированных систем»
название
_____
семестр, учебный год</td><td>Экзаменационный билет №
по дисциплине
МДК 02.01
название
для направления подготовки/ специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем
код, название
технический
профиль/специализация</td><td>«Утверждаю»
Председатель ПЦК
_____
ФИО
«___» _____ 20 __ г.</td></tr>
<tr><td colspan="3">1. Аппаратные устройства для разграничения доступа в сети. (ОК 01, ОК 02, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6)</td></tr>
<tr><td colspan="3">2. DNS имя: назначение, структура, применение (ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6)</td></tr>
<tr><td colspan="3">3. Утилита "Диспетчер задач": назначение, функции. (ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3)</td></tr>
</table>

3. Тестовые задания. Оценка по результатам тестирования.

3.1. Примерные задания теста по МДК 02.01 к другим формам промежуточной аттестации.
Компетенции ОК 01, ОК 02, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6
1. Возможность за приемлемое время получить требуемую информационную услугу называется:
- Конфиденциальность
- Доступность
- Целостность
- Непрерывность

2. К аспектам информационной безопасности не относится:

- Доступность
- Целостность
- Конфиденциальность
- Защищенность

3. По каким критериям нельзя классифицировать угрозы:
   - по расположению источника угроз
   - по аспекту информационной безопасности, против которого угрозы направлены в первую очередь
   - по способу предотвращения
   - по компонентам информационных систем, на которые угрозы нацелены

4. Главное достоинство парольной аутентификации – …
   - простота
   - надежность
   - секретность
   - запоминаемость

5. Сколько уровней включает в себя сетевая модель OSI?
   - 5
   - 7
   - 6
   - 8

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6

6. Межсетевой экран (Брандмауэр, firewall) – это…
   - Комплекс аппаратных средств
   - Комплекс программных средств
   - Комплекс аппаратных или программных средств
   - Комплекс аппаратных и программных средств

7. На каком уровне сетевой модели OSI не работает межсетевой экран:
   - Физический
   - Сеансовый
   - Сетевой
   - Транспортный

8. Межсетевого экрана какого класса не существует:
   - экранирующий маршрутизатор
   - экранирующий коммутатор
   - экранирующий транспорт
   - экранирующий шлюз

9. Что из перечисленного не входит в состав программного комплекса антивирусной защиты:
   - Подсистема сканирования
   - Подсистема управления
   - Подсистема обнаружения вирусной активности
   - Подсистема устранения вирусной активности

10. На каком этапе заканчивается жизненный цикл автоматизированной системы?
    - Бета-тестирование системы
    - Внедрение финальной версии системы в эксплуатацию
    - Прекращение сопровождения и технической поддержки системы
    - Альфа-тестирование системы

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3

11. Какие задачи выполняет теория защиты информации:
    - предоставлять полные и адекватные сведения о происхождении, сущности и развитии проблем защиты
    - аккумулировать опыт предшествующего развития исследований, разработок и практического решения задач защиты информации
    - формировать научно обоснованные перспективные направления развития теории и практики защиты информации
    - выполняет все вышеперечисленные

12. Какой из протоколов не относится к протоколам защищенной передачи данных в сети Интернет:
    - SSL
    - SET
    - HTTP
    - IPSec

13. Какого метода разграничения доступа не существует:
- разграничение доступа по спискам
- разграничение доступа по уровням секретности и категориям
- локальное разграничение доступа
- парольное разграничение доступа

14. К основным функциям подсистемы защиты операционной системы относятся:
- идентификация, аутентификация, авторизация, управление политикой безопасности и разграничение доступа
- криптографические функции
- сетевые функции
- все вышеперечисленные

15. Риск – это…
- вероятностная оценка величины возможного ущерба, который может понести владелец информационного ресурса в результате успешно проведенной атаки
- фактическая оценка величины ущерба, который понес владелец информационного ресурса в результате успешно проведенной атаки
- действие, которое направлено на нарушение конфиденциальности, целостности и/или доступности информации, а также на нелегальное использование других ресурсов сети
- реализованная угроза

3.2. Примерные задания теста по МДК 02.01 к зачету.
Компетенции ОК 01, ОК 02, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6

1. Под угрозой безопасности информации в компьютерной системе (КС) понимают:
a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.
b) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.
c) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

2. Уязвимость информации — это:
a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.
b) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.
c) это действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

3. Атакой на КС называют:
a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.
b) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.
c) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

4. Искусственные угрозы исходя из их мотивов разделяются на:
a) непреднамеренные и преднамеренные
b) косвенные и непосредственные
c) несанкционированные и санкционированные

5. К непреднамеренным угрозам относятся:
a) ошибки в разработке программных средств КС
b) несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями.
c) угроза нарушения конфиденциальности, т.е. утечки информации ограниченного доступа, хранящейся в КС или передаваемой от одной КС к другой;

6. К умышленным угрозам относятся:
a) несанкционированные действия обслуживающего персонала КС (например, ослабление политики безопасности администратором, отвечающим за безопасность КС);

b) воздействие на аппаратные средства КС физических полей других электронных устройств (при несоблюдении условий их электромагнитной совместимости) и др.
c) ошибки пользователей КС;

7. Косвенными каналами утечки называют:
a) каналы, не связанные с физическим доступом к элементам КС
b) каналы, связанные с физическим доступом к элементам КС
c) каналы, связанные с изменение элементов КС и ее структуры.

8. К косвенным каналам утечки информации относятся:
a) использование подслушивающих (радиозакладных) устройств;
b) маскировка под других пользователей путем похищения их идентифицирующей информации (паролей, карт и т.п.);
c) злоумышленное изменение программ для выполнения ими несанкционированного копирования информации при ее обработке;

9. Непосредственными каналами утечки называют:
a) каналы, связанные с физическим доступом к элементам КС.
b) каналы, не связанные с физическим доступом к элементам КС
c) каналы, связанные с изменение элементов КС и ее структуры.

10. К непосредственным каналам утески информации относятся:
a) обход средств разграничения доступа к информационным ресурсам вследствие недостатков в их программном обеспечении и др.
b) перехват побочных электромагнитных излучений и наводок (ПЭМИН).
c) дистанционное видеонаблюдение;

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3
11. Избирательная политика безопасности подразумевает, что:
a) права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).
b) все субъекты и объекты системы должны быть однозначно идентифицированы;
c) каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации;

12. Полномочная политика безопасности подразумевает, что:
a) каждому субъекту системы присвоен уровень прозрачности (security clearance), определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.
b) все субъекты и объекты системы должны быть идентифицированы;
c) права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).

13. Достоверная вычислительная база - это:
a) абстрактное понятие, обозначающее полностью защищенный механизм вычислительной системы (включая аппаратные и программные средства), отвечающий за поддержку реализации политики безопасности.
b) активный компонент системы, который может явиться причиной потока информации от объекта к объекту или изменения состояния системы.
c) пассивный компонент системы, хранящий, принимающий или передающий информацию.

14. Достоверная вычислительная база выполняет задачи:
a) поддерживает реализацию политики безопасности и является гарантом целостности механизмов защиты
b) функционирует на фоне избирательной политики, придавая ее требованиям иерархически упорядоченный характер (в соответствии с уровнями безопасности)
c) представляет собой некоторый соответствующую проверку, организационных мер набор требований, прошедших реализуемых при помощи

15. Уязвимость информации — это:
a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.
b) набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа.

c) неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения.

16. Идентификация объекта - это:
a) одна из функций подсистемы защиты.
b) взаимное установление подлинности объектов, связывающихся между собой по линиям связи.
c) сфера действий пользователя и доступные ему ресурсы КС

17. Процедуру установки сфер действия пользователя и доступные ему ресурсы КС называют:
a) авторизацией
b) аутентификацией
c) Идентификация

18. Авторизация - это:
a) предоставлением полномочий
b) подтверждение подлинности
c) цифровая подпись

19. Аутентификация – это:
a) подтверждение подлинности
b) предоставлением полномочий
c) цифровая подпись

20. Биометрическая идентификация и аутентификация пользователя это:
a) идентификация потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения.
b) схема идентификации позволяющая увеличить число аккредитаций, выполняемых за один цикл, и тем самым уменьшить длительность процесса идентификации.
c) схема идентификации с нулевой передачей знаний.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6
21. Для чего используется процедура «рукопожатия»:
a) для взаимной проверки подлинности
b) для распределения ключей между подлинными партнерами
c) для безопасного использования интеллектуальных карт

22. Параллельная схема идентификации позволяет увеличить:
a) число аккредитаций, выполняемых за один цикл, и тем самым уменьшить длительность процесса идентификации.
b) регистрацию времени для каждого сообщения
c) объект-эталон для идентификации и аутентификации пользователей

23. Внешняя и внутренняя формы представления аутентифицирующего объекта должны быть:
a) семантически тождественны
b) модифицированы
c) структурированы

24. Для чего были разработаны протоколы идентификации с нулевой передачей знаний:
a) для безопасного использования интеллектуальных карт
b) для взаимной проверки подлинности
c) для распределения ключей между подлинными партнерами

25. Механизм запроса-ответа используется для:
a) проверки подлинности
b) шифрования
c) регистрации времени для каждого сообщения

26. Кто разработал алгоритм идентификации с нулевой передачей знания:
a) Гиллоу и Ж. Куискуотером
b) У. Фейге
c) А. Фиат и А. Шамир

27. Схему идентификации с нулевой передачей знаний предложили:
a) У. Фейге, А. Фиат и А. Шамир
b) Гиллоу и Ж. Куискуотером
c) А. Фиат и А. Шамир

28. Для чего создается система разграничения доступа к информации:
a) для защиты информации от НСД
b) для осуществления НСДИ
c) определения максимального уровня конфиденциальности документа

29. Какие методы организации разграничения доступа используются в КС: a) матричный
b) структурированный
c) метод Гиллоу-Куискуотера

30. Мандатный метод основывается на:
a) многоуровневой модели защиты
b) использование матриц доступа
c) криптографическом преобразовании

3.2. Примерные задания теста по МДК 02.01 к экзамену.
Компетенции ОК 01, ОК 02, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6

1. Какой из функциональных блоков должна содержать система разграничения доступа к информации:
a) блок криптографического преобразования информации при ее хранении и передаче;
b) блок контроля среды размещения
c) блок контроля среды выполнения.

2. Диспетчер доступа реализуется в виде:
a) аппаратно-программных механизмов
b) аппаратных механизмов
c) программных механизмов

3. Под ядром безопасности понимают:
a) локализованную, минимизированную, четко ограниченную и надежно изолированную совокупность программно-аппаратных механизмов, доказательно правильно реализующих функции диспетчера доступа.
b) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.
c) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

4. Главным условием создания ядра безопасности является:
a) обеспечение многоуровневого режима выполнения команд
b) мандатное управление
c) Матричная структура

5. Под организацией доступа к ресурсам понимается
a) весь комплекс мер, который выполняется в процессе эксплуатации КС для предотвращения несанкционированного воздействия на технические и программные средства, а также на информацию.
b) хранения атрибутов системы защиты, поддержки криптографического закрытия информации, обработки сбоев и отказов и некоторые другие.
c) предотвращение несанкционированного перехода пользовательских процессов в привилегированное состояние

6. При эксплуатации механизмов аутентификации основными задачами являются:
a) генерация или изготовление идентификаторов, их учет и хранение, передача идентификаторов пользователю и контроль над правильностью выполнения процедур аутентификации в КС.
b) разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц;
c) реализация механизма виртуальной памяти с разделением адресных пространств;

7. В чем заключается правило разграничения доступа

a) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа равен или выше уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа.
b) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа ниже уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа.
c) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа ниже уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа,не содержатся все категории, определенные для данного документа.

8. Правильность функционирования ядра безопасности доказывается путем:
a) полной формальной верификации его программ и пошаговым доказательством их соответствия выбранной математической модели защиты.
b) использования дополнительных программных или аппаратно-программных средств.
c) использования строго определенного множества программ.

9. Матричное управление доступом предполагает использование:
a) матриц доступа
b) аппаратно-программных механизмов
c) субъекта допуска

10. Основной проблемой создания высокоэффективной защиты от НСД является
a) предотвращение несанкционированного перехода пользовательских процессов в привилегированное состояние.
b) использования дополнительных программных или аппаратно-программных средств.
c) разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3
11. Аппаратно-программмные средства криптографической защиты информации выполняют функции:
a) аутентификацию пользователя, разграничение доступа к информации, обеспечение целостности информации и ее защиты от уничтожения, шифрование и электронную цифровую подпись.
b) организовывают реализацию политики безопасности информации на этапе эксплуатации КС.
c) проверяют на отсутствие закладок приборов, устройств.

12. Использование аппаратных средств снимает проблему:
a) обеспечения целостности системы.
b) разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц
c) использования строго определенного множества программ.

13. Криптографические функции плат КРИПТОН образующие ядро системы безопасности реализуются
a) аппаратно
b) программно
c) аппаратно и программно

14. Безопасность в частично контролируемым компьютерных системамах может быть обеспечена
a) изоляцией от злоумышленника ненадежной компьютерной среды, отдельного ее компонента или отдельного процесса с помощью полностью контролируемых средств.
b) схемой идентификации позволяющая увеличить число аккредитаций, выполняемых за один цикл, и тем самым уменьшить длительность процесса идентификации.
c) внешней аутентификацией объекта, не принадлежащего системе;

15. Платы серии КРИПТОН, обеспечивают защиту:
a) ключей шифрования и электронной цифровой подписи (ЭЦП), так и неизменность их алгоритмов.
b) аппаратно-программных механизмов
c) реализации механизма виртуальной памяти с разделением адресных пространств;

16. К основным компонентам сети относятся:
a) центры коммутации пакетов, маршрутизаторы, шлюзы и сетевые экраны;

b) субъекты доступа
c) платы серии КРИПТОН

17. В качестве ключевых носителей устройств криптографической защиты данных серии КРИПТОН используются:
a) дискеты, смарт-карты и Touch-Memory.
b) смарт-карты, Touch-Memory
c) дискеты, смарт-карты

18. Средства серии КРИПТОН независимо от операционной среды обеспечивают:
a) защиту ключей шифрования и электронной цифровой подписи (ЭЦП) и неизменность алгоритма шифрования и ЭЦП.
b) криптомаршрутизацию
c) функции шифрования и электронной цифровой подписи.

19. В системе Secret Disk используется:
a) смешанная программно-аппаратная схема защиты с возможностью выбора
b) реализация механизма виртуальной памяти с разделением адресных пространств;
c) механизм RUN-файлов позволяет в процессе работы запускать любые программы с предварительной проверкой их целостности.

20. В чем заключается особенность системы Secret Disk:
a) для доступа к защищенной информации необходим не только вводимый пользователем пароль, но и электронный идентификатор.
b) для доступа к защищенной информации необходим только вводимый пользователем пароль.
c) для доступа к защищенной информации необходим только электронный идентификатор.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6
21. Мастер-ключ в Устройствах криптографической защиты данных серии КРИПТОН загружается:
a) до загрузки операционной системы
b) после загрузки операционной системы
c) вообще не загружается

22. Криптографических функций в устройствах криптографической защиты данных серии КРИПТОН выполняются:
a) внутри платы
b) в операционной системе
c) в блоке загрузки операционной системы

23. Под защитой информации понимается
a) совокупность мероприятий, методов и средств, обеспечивающих решение следующих задач по проверке целостности информации и исключении несанкционированного доступа к ресурсам ПЭВМ и хранящимся в ней программам и данным.
b) совокупность мероприятий, методов и средств, обеспечивающих решение следующих задач по реализации механизма виртуальной памяти с разделением адресных пространств;
c) совокупность мероприятий, методов и средств, обеспечивающих решение следующих задач по разграничению прав пользователей и обслуживающего персонала.

24. Возможные каналы утечки информации по классификации разделяют:
a) человек, аппаратура, программа
b) человек, линия связи
c) коммутационное оборудование, человек

25. К группе каналов утечки информации в которой основным средством является человек, относятся следующие утечки:
a) расшифровка программой зашифрованной информации;
b) несанкционированный доступ программы к информации;
c) копирование программой информации с носителей.

26. К группе каналов утечки информации в которой основным средством является аппаратура, относятся следующие утечки:
a) подключение к ПЭВМ специально разработанных аппаратных средств, обеспечивающих доступ к информации;
b) хищение носителей информации (магнитных дисков, дискет, лент)

c) копирование программой информации с носителей

27. К группе каналов утечки информации в которой основным средством является программа, относятся следующие утечки:
a) несанкционированный доступ программы к информации
b) хищение носителей информации (магнитных дисков, дискет, лент)
c) использование специальных технических средств для перехвата электромагнитных излучений технических средств ПЭВМ.

28. К средствам активной защиты относятся:
a) искаженные программы (программы вирусы, искажение функций)
b) заказное проектирование
c) специальная аппаратура

29. К средствам пассивной защиты относятся:
a) частотный анализ
b) авторская эстетика
c) аппаратура защиты (ПЗУ, преобразователи)

3.4. Соответствие между бальной системой и системой оценивания по результатам тестирования устанавливается посредством следующей таблицы:

Объект оценки	Показатели оценивания результатов обучения	Оценка	Уровень результатов обучения
Обучающийся	60 баллов и менее	«Неудовлетворительно» (Не зачтено)	Низкий уровень
	74 – 61 баллов	«Удовлетворительно» (Зачтено)	Пороговый уровень
	84 – 75 баллов	«Хорошо» (Зачтено)	Повышенный уровень
	100 – 85 баллов	«Отлично» (Зачтено)	Высокий уровень

4. Оценка ответа обучающегося на вопросы.
4.1 Оценка ответа обучающегося на вопросы при защите курсового проекта

Элементы оценивания	Содержание шкалы оценивания			
	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
Соответствие содержания КП методике расчета (исследования)	Полное несоответствие содержания КП поставленным целям или их отсутствие	Значительные погрешности	Незначительные погрешности	Полное соответствие
Качество обзора литературы	Недостаточный анализ	Отечественная литература	Современная отечественная литература	Новая отечественная и зарубежная литература
Творческий характер КП, степень самостоятельности в разработке	Работа в значительной степени не является самостоятельной	В значительной степени в работе использованы выводы, выдержки из других авторов без ссылок на них	В ряде случае отсутствуют ссылки на источник информации	Полное соответствие критерию
Использование современных информационных технологий	Современные информационные технологии, вычислительная техника не были использованы	Современные информационные технологии, вычислительная техника использованы слабо. Допущены серьезные ошибки в расчетах	Имеют место небольшие погрешности в использовании современных информационных технологий, вычислительной техники	Полное соответствие критерию
Качество графического материала в КП	Не раскрывают смысл работы, небрежно оформлено, с большими	Не полностью раскрывают смысл, есть существенные погрешности в	Не полностью раскрывают смысл, есть погрешность в оформлении	Полностью раскрывают смысл и отвечают ГОСТ, ЕСКД и др.

	отклонениями от требований ГОСТ, ЕСКД и др.	оформлении		
Грамотность изложения текста КП	Много стилистических и грамматических ошибок	Есть отдельные грамматические и стилистические ошибки	Есть отдельные грамматические ошибки	Текст КП читается легко, ошибки отсутствуют
Соответствие требованиям, предъявляемым к оформлению КП	Полное не выполнение требований, предъявляемых к оформлению	Требования, предъявляемые к оформлению КП, нарушены	Допущены незначительные погрешности в оформлении КП	КП соответствует всем предъявленным требованиям
Качество доклада	В докладе не раскрыта тема КП, нарушен регламент	Не соблюден регламент, недостаточно раскрыта тема КП	Есть ошибки в регламенте и использовании чертежей	Соблюдение времени, полное раскрытие темы КП
Качество ответов на вопросы	Не может ответить на дополнительные вопросы	Знание основного материала	Высокая эрудиция, нет существенных ошибок	Ответы точные, высокий уровень эрудиции

4.2. Оценка ответа обучающегося на вопросы к другим формам промежуточной аттестации (устному опросу), зачету и экзамену.

Элементы оценивания	Содержание шкалы оценивания			
	Неудовлетворительно (Не зачтено)	Удовлетворительно (Зачтено)	Хорошо (Зачтено)	Отлично (Зачтено)
Соответствие ответов формулировкам вопросов (заданий)	Полное несоответствие по всем вопросам	Значительные погрешности	Незначительные погрешности	Полное соответствие
Структура, последовательность и логика ответа. Умение четко, понятно, грамотно и свободно излагать свои мысли	Полное несоответствие критерию.	Значительное несоответствие критерию	Незначительное несоответствие критерию	Соответствие критерию при ответе на все вопросы.
Знание нормативных, правовых документов и специальной литературы	Полное незнание нормативной и правовой базы и специальной литературы	Имеют место существенные упущения (незнание большей части из документов и специальной литературы по названию, содержанию и т.д.).	Имеют место несущественные упущения и незнание отдельных (единичных) работ из числа обязательной литературы.	Полное соответствие данному критерию ответов на все вопросы.
Умение увязывать теорию с практикой, в том числе в области профессиональной работы	Умение связать теорию с практикой работы не проявляется.	Умение связать вопросы теории и практики проявляется редко.	Умение связать вопросы теории и практики в основном проявляется.	Полное соответствие данному критерию. Способность интегрировать знания и привлекать сведения из различных научных сфер
Качество ответов на дополнительные вопросы	На все дополнительные вопросы преподавателя даны неверные ответы.	Ответы на большую часть дополнительных вопросов преподавателя даны неверно.	1. Даны неполные ответы на дополнительные вопросы преподавателя. 2. Дан один неверный ответ на дополнительные вопросы преподавателя.	Даны верные ответы на все дополнительные вопросы преподавателя.

Примечание: итоговая оценка формируется как средняя арифметическая результатов элементов оценивания.

МДК.02.02 «Криптографические средства защиты информации»

1. Описание показателей, критериев и шкал оценивания компетенций.

1.1. Показатели и критерии оценивания компетенций ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4

Объект оценки	Уровни сформированности компетенций	Критерий оценивания результатов обучения
Обучающийся	Низкий уровень Пороговый уровень Повышенный уровень Высокий уровень	Уровень результатов обучения **не ниже порогового**

1.2. Шкалы оценивания компетенций ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4 при сдаче дифференцированного зачета и экзамена

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания
		Дифференцированный зачет (Экзамен)
Низкий уровень	Обучающийся: -обнаружил пробелы в знаниях основного учебно-программного материала; -допустил принципиальные ошибки в выполнении заданий, предусмотренных программой; -не может продолжить обучение или приступить к профессиональной деятельности по окончании программы без дополнительных занятий по соответствующей дисциплине.	Неудовлетворительно
Пороговый уровень	Обучающийся: -обнаружил знание основного учебно-программного материала в объёме, необходимом для дальнейшей учебной и предстоящей профессиональной деятельности; -справляется с выполнением заданий, предусмотренных программой; -знаком с основной литературой, рекомендованной рабочей программой дисциплины; -допустил неточности в ответе на вопросы и при выполнении заданий по учебно-программному материалу, но обладает необходимыми знаниями для их устранения под руководством преподавателя.	Удовлетворительно
Повышенный уровень	Обучающийся: - обнаружил полное знание учебно-программного материала; -успешно выполнил задания, предусмотренные программой; -усвоил основную литературу, рекомендованную рабочей программой дисциплины; -показал систематический характер знаний учебно-программного материала; -способен к самостоятельному пополнению знаний по учебно-программному материалу и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.	Хорошо
Высокий уровень	Обучающийся: -обнаружил всесторонние, систематические и глубокие знания учебно-программного материала; -умеет свободно выполнять задания, предусмотренные программой; -ознакомился с дополнительной литературой; -усвоил взаимосвязь основных понятий дисциплин и их значение для приобретения профессии; -проявил творческие способности в понимании учебно-программного материала.	Отлично

1.3. Описание шкал оценивания
Компетенции обучающегося оценивается следующим образом:

Планируемый уровень результатов освоения	Содержание шкалы оценивания достигнутого уровня результата обучения			
	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
Знать	Неспособность обучающегося самостоятельно продемонстрировать наличие знаний при решении заданий,	Обучающийся способен самостоятельно продемонстрировать наличие знаний при решении	Обучающийся демонстрирует способность к самостоятельному применению знаний при	Обучающийся демонстрирует способность к самостоятельному применению знаний в выборе способа

	которые были представлены преподавателем вместе с образцом их решения.	заданий, которые были представлены преподавателем вместе с образцом их решения.	решении заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	решения неизвестных или нестандартных заданий и при консультативной поддержке в части междисциплинарных связей.
Уметь	Отсутствие у обучающегося самостоятельности в применении умений по использованию методов освоения учебной дисциплины.	Обучающийся демонстрирует самостоятельность в применении умений решения учебных заданий в полном соответствии с образцом, данным преподавателем.	Обучающийся продемонстрирует самостоятельное применение умений решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение умений решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.
Иметь практический опыт	Неспособность самостоятельно проявить навык решения поставленной задачи по стандартному образцу повторно.	Обучающийся демонстрирует самостоятельность в применении навыка по заданиям, решение которых было показано преподавателем.	Обучающийся демонстрирует самостоятельное применение навыка решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение навыка решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.

2. Перечень вопросов к дифференцированному зачету и экзамену.

2.1 Примерный перечень вопросов к дифференцированному зачету.
Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4

1. Основная теорема арифметики. Взаимно простые числа и функция Эйлера. Простые числа Ферма.
2. Малая теорема Ферма. Теорема Ферма-Эйлера.
3. Китайская теорема об остатках.
4. Шифры потока и блочные шифры. Основные принципы. Определения.
5. Современные блочные шифры. Основные принципы. Определения.
6. Понятие: подстановка, транспозиция и полноразмерный ключевой шифр.

Компетенции ОК 01, ОК 5, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4

7. Компоненты современного блочного шифра. Понятие: P-блоки и S-блоки. Алгоритм. Виды. Назначение. Раунды.
8. Компоненты современного блочного шифра.
9. Операция циклического сдвига. Операция замены.
10. Разбиение и объединение. Рассеивание и перемешивание.
11. Шифр Файстеля и шифр не-Файстеля. Основная идея. Алгоритм. Криптоанализ.
12. Современные шифры потока. Основные принципы. Определения.
13. Стандарт шифрования данных DES (DATA ENCRYPTION STAND-ARD). Основная идея. Алгоритм. Криптоанализ.
14. Стандарт шифрования данных AES (ADVANCED ENCRYPTION STANDARD). Основная идея. Алгоритм. Криптоанализ.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 5, ОК 06, ПК 2.4

15. Алгоритм криптографического преобразования данных ГОСТ 28147-89. Основная идея. Алгоритм. Криптоанализ.
16. Решение линейного уравнения с одним неизвестным, вида: $ax=b(\mathrm{mod}\ n)$.
17. Решение системы линейных уравнений.
18. Алгебраические структуры. Группа. Циклическая группа. Кольцо. Поле.
19. Конечные поля. Поля Галуа. Полиномы.
20. Понятие хеш-функции. Основные требования, предъявляемые к криптографическим хеш-функциям.

2.2 Примерный перечень вопросов к экзамену. Образец экзаменационного билета.

2.2.1 Примерный перечень вопросов к экзамену.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4

1. Генераторы псевдослучайных чисел.
2. Основные принципы использования генераторов псевдослучайных чисел при потоковом шифровании.
3. Шифры потока и блочные шифры. Основные принципы. Определения.
4. Современные блочные шифры. Основные принципы. Определения.
5. Понятие: подстановка, транспозиция и полноразмерный ключевой шифр.
6. Компоненты современного блочного шифра.
7. Понятие: P-блоки и S-блоки. Алгоритм. Виды. Назначение. Раунды.
8. Компоненты современного блочного шифра. Операция циклического сдвига. Операция замены.

Компетенции ОК 01, ОК 5, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4

9. Разбиение и объединение. Рассеивание и перемешивание.
10. Шифр Файстеля и шифр не-Файстеля. Основная идея. Алгоритм. Криптоанализ.
11. Современные шифры потока. Основные принципы. Определения.
12. Стандарт шифрования данных DES (DATA ENCRYPTION STAND-ARD). Основная идея. Алгоритм. Криптоанализ.
13. Стандарт шифрования данных AES (ADVANCED ENCRYPTION STANDARD). Основная идея. Алгоритм. Криптоанализ.
14. Алгоритм криптографического преобразования данных ГОСТ 28147-89. Основная идея. Алгоритм. Криптоанализ.
15. Ранцевая криптографическая система. Основная идея. Алгоритм. Криптоанализ.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 5, ОК 06, ПК 2.4

16. Криптографическая система RSA. Основная идея. Алгоритм. Криптоанализ.
17. Алгоритм Диффи-Хеллмана. Основная идея. Алгоритм. Криптоанализ.
18. Алгоритм Рабина. Основная идея. Алгоритм. Криптоанализ
19. Алгоритм Эль-Гамаля. Основная идея. Алгоритм. Криптоанализ.
20. Стандарты на алгоритмы цифровой подписи: DSS (Digital Signature Standard), ГОСТ Р34.10-94 и ГОСТ Р34.10-2001. Основная идея. Алгоритм. Криптоанализ.
21. Алгоритм шифрования RC4. Основная идея. Алгоритм. Криптоанализ.
22 Криптосистемы на основе эллиптических уравнений. Основная идея. Алгоритм. Криптоанализ.
23. Совершенно секретные криптографические системы. Основные подходы.
24. Экономика информационной безопасности на примере оценки криптосистем.

2.2.2. Образец экзаменационного билета по МДК 02.02

<table>
<tr><td colspan="3">Дальневосточный государственный университет путей сообщения</td></tr>
<tr><td>ПЦК
«Информационная безопасность автоматизированных систем»
название
_____
семестр, учебный год</td><td>Экзаменационный билет №
по дисциплине
_____МДК 02.02_____
название
для направления подготовки/ специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем
код, название
технический
профиль/специализация</td><td>«Утверждаю»
Председатель ПЦК
_____
ФИО
«___» _____ 20 __ г.</td></tr>
<tr><td colspan="3">1. Компоненты современного блочного шифра. Операция циклического сдвига. Операция замены. (ОК 01, ОК 02, ОК 03, ОК 04, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4)</td></tr>
<tr><td colspan="3">2. Современные шифры потока. Основные принципы. Определения. (ОК 01, ОК 5, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4)</td></tr>
<tr><td colspan="3">3. Алгоритм шифрования RC4. Основная идея. Алгоритм. Криптоанализ (ОК 01, ОК 02, ОК 03, ОК 04, ОК 5, ОК 06, ПК 2.4)</td></tr>
</table>

3. Тестовые задания. Оценка по результатам тестирования.

3.1. Примерные задания теста по МДК 02.02 к дифференцированному зачету

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4

1. Происхождение термина «криптография»:
   - от слова «тайнопись»;
   - от слова «шифрование»;
   - от термина «скремблирование»;
   - от термина «кодирование»;

2. Метод надежной передачи информации по открытому каналу связи использует:
- криптографию;
- стеганографию;
- кодирование;
- скремблирование;

3. Для чего используется система Kerberos?
- для симметричной аутентификации;
- для несимметричной аутентификации;
- для выработки ЭЦП;
- для шифрования;

4. Что такое код обнаружения манипуляции с данными MDC?
- есть результат действия хэш-функции;
- циклический контрольный код сообщения;
- код четности;
- имитоприставка;

5. Наука об обеспечении секретности и / или аутентичности (подлинности) передаваемых сообщений:
- ЭЦП;
- криптография;
- криптоанализ;
- стеганография;

6. Замену символов с открытого текста, соответствующими символами алфавита криптотекста называют:
- простейшим шифром;
- блочным шифром;
- шифром подстановки;
- шифром замены;

7. Функции, для которых легко найти функцию прямого отображения и нельзя найти обратное называются:
- линейные функции;
- нелинейные функции;
- односторонние функции;
- функции преобразования;

Компетенции ОК 01, ОК 5, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4

8. Системы, где с помощью открытого ключа шифруют ключ блочного криптоалгоритма, а само сообщение шифруют с помощью этого симметричного секретного ключа, называют:
- гибридные криптосистемы;
- криптосистема RSA;
- электронная подпись;
- криптографические протоколы;

9. Как называют в ГОСТе режим электронной кодовой книги (ECB):
- режим сцепления блоков шифротекста;
- режим простой замены;
- режим обратных связей по выбору;
- режим счетчика;

10. Процесс применения шифра защищаемой информации называют:
- дешифрованием;
- вскрытием шифра;
- простой заменой;
- шифрованием;

11. Как называют в криптографии сменный элемент шифра, который применяется для шифрования конкретного сообщения:
- ключ;
- разрядность блока;
- число раундов шифрования;
- алгоритм шифрования;

12. Процесс наложения по определенному закону гамма-шифра на открытые данные:
- хэширование;
- имитовставка;
- гаммирование;
- ЭЦП;

13. Шифр – это …
- ключевое запоминающее устройство;
- совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с использованием ключей;
- состояние, выражающее процесс образования зашифрованных данных из открытых данных;
- значение исходных открытых параметров алгоритма криптографического преобразования;

14. Разрядность 3DES равна:
- 56 бит;
- 112 бит;
- 168 бит;
- 256 бит;

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 5, ОК 06, ПК 2.4

15. При использовании классических криптографических алгоритмов ключ шифрования и ключ дешифрования совпадают и такие криптосистемы называются:
- простыми криптосистемами;
- гибридными криптосистемами;
- ассиметричными криптосистемами;
- симметричными криптосистемами;

16. Линейное шифрование данных , основанное на поточном способе шифрования называется:
- гаммированием;
- подстановкой;
- перестановкой;
- имитовставкой;

17. Криптографическая система открытого ключа, обеспечивающая такие механизмы защиты как шифрование и цифровая подпись, разработанная в 1977 году, называется:
- алгоритм шифрования RSA;
- алгоритм DSA;
- алгоритм DSS;
- алгоритм SHA;

18. Цифровая подпись - …
- подпись, которая ставится на документах;
- небольшое количество дополнительной цифровой информации, передаваемое вместе с подписываемым текстом, по которому можно удостоверится в аутентичности документа;
- код с исправлением ошибок;
- имитоприставка;

19. Функция, предназначенная для сжатия подписываемого документа до нескольких десятков, или сотен бит называется:
- логарифмической функцией;
- тригонометрической функцией;
- хэш- функцией;
- ЭЦП;

20. Этот алгоритм был разработан НИСТ и АНБ США в рамках стандарта безопасного хэширования SHS в 1992 году и предназначен для использования совместно с алгоритмом цифровой подписи DSA:
- DES;
- ГОСТ;
- Rundjael;
- SHA;

21. Чему равна разрядность блока алгоритма шифрования DES:
- 56 битам;
- 128 битам;
- 64 битам;
- 256 битам;

3.2. Примерные задания теста по МДК 02.02 к экзамену

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4

1. Цель атаки на криптосистему:
- нарушение целостности передачи информации абоненту;
- вскрытие ключа шифрования;
- фальсификация сообщения;

- вскрытие передаваемых зашифрованных сообщений;

2. Криптосистемы с последовательным выполнением преобразований над элементами открытого текста называется:
- поточными шифрами;
- двоичными аддитивными шифрами;
- блочными шифрами;
- криптосистемами с ключом однократного применения;

3.Установление санкционированным получателем (приемником) того факта, что полученное сообщение послано санкционированным отправителем (передатчиком) называется:
- идентификацией;
- аутентификацией;
- авторизацией;
- контролем целостности информации;

4. Разрядность шифруемых блоков данных RSA:
- произвольная;
- меньше разрядности ключа;
- равна разрядности ключа;
- больше разрядности ключа;

5. Совокупность действий (инструкций, команд, вычислений), выполняемых в заданной последовательности двумя или более субъектами с целью достижения определенного результата называется:
- алгоритмом;
- шифрованием;
- дешифрованием;
- протоколом;

6. Какова разрядность ключа алгоритма шифрования ГОСТ 28147 – 89 (первого российского стандарта шифрования):
- 56 бит;
- 64 бит;
- 128 бит;
- 256 бит;

7. Чем отличаются синхронные поточные шифры от блочных шифров?
- шифрограмма есть результат наложения последовательности текста и последовательности работающего генератора гамма;
- шифрограмма есть результат наложения последовательности текста и последовательности гаммы, зависящей от входной последовательности;
- вычисляется ЭЦП;
- дополняется хэш-функцией;

8. Чем отличаются самосинхронизирующие поточные шифры от блочных шифров?
- шифрограмма есть результат наложения последовательности текста и последовательности работающего генератора гамма;
- шифрограмма есть результат наложения последовательности текста и последовательности гаммы, зависящей от входной последовательности;
- вычисляется ЭЦП;
- дополняется хэш-функцией;

9. Почему так широко используют циклы Фейштеля в криптографии?
- упрощается процесс дешифрования;
- получается абсолютно-стойкий шифр;
- из-за известности имени Фейштеля;
- не требуется аутентификация;

Компетенции ОК 01, ОК 5, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.4

10. В чем состоит задача криптографа?
- взломать систему защиты
- обеспечить конфиденциальность и аутентификацию передаваемых сообщений

11. Верификация – это
- это проверка принадлежности субъекту доступа предъявленного им идентификатора.
- проверка целостности и подлинности инф, программы, документа
- это присвоение имени субъекту или объекту

12. Кодирование информации – это

- представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д.
- метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом

13. Наука о скрытой передаче информации путем сохранения в тайне самого факта передачи – это
    - Стенография
    - Криптография
    - Криптоанализ

14. Линейное шифрование –
    - несанкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу
    - криптографическое преобразование информации при ее передаче по прямым каналам связи от одного элемента ВС к другому
    - криптографическое преобразование информации в целях ее защиты от ознакомления и модификации посторонними лицами

15. Подпись называется детерминированной, если
    - для одного и того же сообщения с использованием разных закрытых ключей при каждом подписывании создается одна и та же подпись
    - для разных сообщений с использованием одного и того закрытого ключа при каждом подписывании создается одна и та же подпись
    - для одного и того же сообщения с использованием одного и того же закрытого ключа при каждом подписывании создается одна и та же подпись

16. Подпись называется рандомизированной, если
    - для разных сообщений с использованием одного и того же закрытого ключа при каждом подписывании создаются разные подписи
    - для одного и того же сообщения с использованием одного и того же закрытого ключа при каждом подписывании создаются разные подписи
    - для одного и того же сообщения с использованием разных закрытых ключей при каждом подписывании создаются разные подписи

17. Подпись, создаваемая DSS, является
    - детерминированной
    - рандомизированной

18. Подпись, создаваемая RSA, является
    - детерминированной
    - рандомизированной

19. Подпись, создаваемая ГОСТ 3410, является
    - детерминированной
    - рандомизированной

20. Длина хэш-кода хэш-функции ГОСТ 3411 равна
    - 128 бит
    - 160 бит
    - 256 бит

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 5, ОК 06, ПК 2.4

21. Последовательность случайных чисел должна быть
    - монотонно возрастающей
    - монотонно убывающей
    - иметь равномерное распределение

22. В DSS используется следующая хэш-функция
    - MD5
    - SHA-1
    - SHA-2

23. Алгоритм MARS обладает следующими свойствами
    - имеет самое быстрое установление ключа
    - имеет самое быстрое шифрование/дешифрование
    - имеет возможность вычисления подключей на лету
    - шифрование и дешифрование имеют идентичные функции

24. Алгоритм IDEA

- имеет переменную длину ключа
- основан на сети Фейштеля
- разбивает блок на фиксированные 16-битные подблоки

25. Алгоритм ГОСТ 28147
- имеет переменную длину ключа
- основан на сети Фейстеля
- разбивает блок на фиксированные 16-битные подблоки

26. Алгоритм Twofish обладает следующим свойством
- имеет самое быстрое установление ключа
- имеет самое быстрое шифрование/дешифрование
- имеет возможность вычисления подключей на лету

3.3. Соответствие между бальной системой и системой оценивания по результатам тестирования устанавливается посредством следующей таблицы:

Объект оценки	Показатели оценивания результатов обучения	Оценка	Уровень результатов обучения
Обучающийся	60 баллов и менее	«Не удовлетворительно»	Низкий уровень
	74 – 61 баллов	«Удовлетворительно»	Пороговый уровень
	84 – 75 баллов	«Хорошо»	Повышенный уровень
	100 – 85 баллов	«Отлично»	Высокий уровень

4. Оценка ответа обучающегося на вопросы.

4.1. Оценка ответа обучающегося на вопросы к дифференцированному зачету и экзамену.

Элементы оценивания	Содержание шкалы оценивания			
	Не удовлетворительно	Удовлетворительно	Хорошо	Отлично
Соответствие ответов формулировкам вопросов (заданий)	Полное несоответствие по всем вопросам	Значительные погрешности	Незначительные погрешности	Полное соответствие
Структура, последовательность и логика ответа. Умение четко, понятно, грамотно и свободно излагать свои мысли	Полное несоответствие критерию.	Значительное несоответствие критерию	Незначительное несоответствие критерию	Соответствие критерию при ответе на все вопросы.
Знание нормативных, правовых документов и специальной литературы	Полное незнание нормативной и правовой базы и специальной литературы	Имеют место существенные упущения (незнание большей части из документов и специальной литературы по названию, содержанию и т.д.).	Имеют место несущественные упущения и незнание отдельных (единичных) работ из числа обязательной литературы.	Полное соответствие данному критерию ответов на все вопросы.
Умение увязывать теорию с практикой, в том числе в области профессиональной работы	Умение связать теорию с практикой работы не проявляется.	Умение связать вопросы теории и практики проявляется редко.	Умение связать вопросы теории и практики в основном проявляется.	Полное соответствие данному критерию. Способность интегрировать знания и привлекать сведения из различных научных сфер
Качество ответов на дополнительные вопросы	На все дополнительные вопросы преподавателя даны неверные ответы.	Ответы на большую часть дополнительных вопросов преподавателя даны неверно.	1. Даны неполные ответы на дополнительные вопросы преподавателя. 2. Дан один неверный ответ на дополнительные вопросы преподавателя.	Даны верные ответы на все дополнительные вопросы преподавателя.

Примечание: итоговая оценка формируется как средняя арифметическая результатов элементов оценивания.

ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами»

1. Описание показателей, критериев и шкал оценивания компетенций.

1.1. Показатели и критерии оценивания компетенций ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6

Объект оценки	Уровни сформированности компетенций	Критерий оценивания результатов обучения
Обучающийся	Низкий уровень Пороговый уровень Повышенный уровень Высокий уровень	Уровень результатов обучения **не ниже порогового**

1.2. Шкалы оценивания компетенций ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6 при сдаче квалификационного экзамена

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания
		Экзамен
Низкий уровень	Обучающийся: -обнаружил пробелы в знаниях основного учебно-программного материала; -допустил принципиальные ошибки в выполнении заданий, предусмотренных программой; -не может продолжить обучение или приступить к профессиональной деятельности по окончании программы без дополнительных занятий по соответствующей дисциплине.	Неудовлетворительно
Пороговый уровень	Обучающийся: -обнаружил знание основного учебно-программного материала в объёме, необходимом для дальнейшей учебной и предстоящей профессиональной деятельности; -справляется с выполнением заданий, предусмотренных программой; -знаком с основной литературой, рекомендованной рабочей программой дисциплины; -допустил неточности в ответе на вопросы и при выполнении заданий по учебно-программному материалу, но обладает необходимыми знаниями для их устранения под руководством преподавателя.	Удовлетворительно
Повышенный уровень	Обучающийся: - обнаружил полное знание учебно-программного материала; -успешно выполнил задания, предусмотренные программой; -усвоил основную литературу, рекомендованную рабочей программой дисциплины; -показал систематический характер знаний учебно-программного материала; -способен к самостоятельному пополнению знаний по учебно-программному материалу и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.	Хорошо
Высокий уровень	Обучающийся: -обнаружил всесторонние, систематические и глубокие знания учебно-программного материала; -умеет свободно выполнять задания, предусмотренные программой; -ознакомился с дополнительной литературой; -усвоил взаимосвязь основных понятий дисциплин и их значение для приобретения профессии; -проявил творческие способности в понимании учебно-программного материала.	Отлично

1.3. Описание шкал оценивания
Компетенции обучающегося оценивается следующим образом:

Планируемый уровень результатов освоения	Содержание шкалы оценивания достигнутого уровня результата обучения			
	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
Знать	Неспособность обучающегося самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся способен самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся демонстрирует способность к самостоятельному применению знаний при решении заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует способность к самостоятельному применению знаний в выборе способа решения неизвестных или нестандартных заданий и при консультативной поддержке в части междисциплинарных связей.
Уметь	Отсутствие у обучающегося самостоятельности в применении умений по использованию методов освоения учебной дисциплины.	Обучающийся демонстрирует самостоятельность в применении умений решения учебных заданий в полном соответствии с образцом, данным преподавателем.	Обучающийся продемонстрирует самостоятельное применение умений решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение умений решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.
Иметь практический опыт	Неспособность самостоятельно проявить навык решения поставленной задачи по стандартному образцу повторно.	Обучающийся демонстрирует самостоятельность в применении навыка по заданиям, решение которых было показано преподавателем.	Обучающийся демонстрирует самостоятельное применение навыка решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение навыка решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.

Примерный перечень вопросов к квалификационному экзамену по ПМ.02.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6

1. Основная теорема арифметики. Взаимно простые числа и функция Эйлера. Простые числа Ферма.
2. Малая теорема Ферма. Теорема Ферма-Эйлера.
3. Китайская теорема об остатках.
4. Шифры потока и блочные шифры. Основные принципы. Определения.
5. Современные блочные шифры. Основные принципы. Определения.
6. Понятие: подстановка, транспозиция и полноразмерный ключевой шифр.
7. Генераторы псевдослучайных чисел.
8. Основные принципы использования генераторов псевдослучайных чисел при потоковом шифровании.
9. Шифры потока и блочные шифры. Основные принципы. Определения.
10. Современные блочные шифры. Основные принципы. Определения.
11. Понятие: подстановка, транспозиция и полноразмерный ключевой шифр.
12. Компоненты современного блочного шифра.
13. Понятие: P-блоки и S-блоки. Алгоритм. Виды. Назначение. Раунды.
14. Компоненты современного блочного шифра. Операция циклического сдвига. Операция замены.

Компетенции ОК 01, ОК 5, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6

15. Компоненты современного блочного шифра. Понятие: P-блоки и S-блоки. Алгоритм. Виды. Назначение. Раунды.

16. Компоненты современного блочного шифра. Операция циклического сдвига. Операция замены.
17. Разбиение и объединение. Рассеивание и перемешивание.
18. Шифр Файстеля и шифр не-Файстеля. Основная идея. Алгоритм. Криптоанализ.
19. Современные шифры потока. Основные принципы. Определения.
20. Стандарт шифрования данных DES (DATA ENCRYPTION STAND-ARD). Основная идея. Алгоритм. Криптоанализ.
21. Стандарт шифрования данных AES (ADVANCED ENCRYPTION STANDARD). Основная идея. Алгоритм. Криптоанализ.
22. Разбиение и объединение. Рассеивание и перемешивание.
23. Шифр Файстеля и шифр не-Файстеля. Основная идея. Алгоритм. Криптоанализ.
24. Современные шифры потока. Основные принципы. Определения.
25. Стандарт шифрования данных DES (DATA ENCRYPTION STAND-ARD). Основная идея. Алгоритм. Криптоанализ.
26. Стандарт шифрования данных AES (ADVANCED ENCRYPTION STANDARD). Основная идея. Алгоритм. Криптоанализ.
27. Алгоритм криптографического преобразования данных ГОСТ 28147-89. Основная идея. Алгоритм. Криптоанализ.
28. Ранцевая криптографическая система. Основная идея. Алгоритм. Криптоанализ.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 5, ОК 06, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6

29. Алгоритм криптографического преобразования данных ГОСТ 28147-89. Основная идея. Алгоритм. Криптоанализ.
30. Решение линейного уравнения с одним неизвестным, вида: ax=b(mod n).
31. Решение системы линейных уравнений.
32. Алгебраические структуры. Группа. Циклическая группа. Кольцо. Поле.
33. Конечные поля. Поля Галуа. Полиномы.
34. Понятие хеш-функции. Основные требования, предъявляемые к криптографическим хеш-функциям.
35. Криптографическая система RSA. Основная идея. Алгоритм. Криптоанализ.
36. Алгоритм Диффи-Хеллмана. Основная идея. Алгоритм. Криптоанализ.
37. Алгоритм Рабина. Основная идея. Алгоритм. Криптоанализ
38. Алгоритм Эль-Гамаля. Основная идея. Алгоритм. Криптоанализ.
39. Стандарты на алгоритмы цифровой подписи: DSS (Digital Signature Standard), ГОСТ Р34.10-94 и ГОСТ Р34.10-2001. Основная идея. Алгоритм. Криптоанализ.
40. Алгоритм шифрования RC4. Основная идея. Алгоритм. Криптоанализ.
41 Криптосистемы на основе эллиптических уравнений. Основная идея. Алгоритм. Криптоанализ.
42. Совершенно секретные криптографические системы. Основные подходы.
43. Экономика информационной безопасности на примере оценки криптосистем.

Образец экзаменационного билета по ПМ.02

<table>
<tr><td colspan="3">Дальневосточный государственный университет путей сообщения</td></tr>
<tr><td>ПЦК
Информационная безопасность автоматизированных систем
название
_____
семестр, учебный год</td><td>Экзаменационный билет №
по ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами
название
для направления подготовки/специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем
код, название
технический
профиль/специализация</td><td>«Утверждаю»
Председатель ПЦК
_____
ФИО
«___» _____ 20 __ г.</td></tr>
<tr><td colspan="3">1. Основные принципы использования генераторов псевдослучайных чисел при потоковом шифровании. (ОК 01, ОК 02, ОК 03, ОК 04, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6)</td></tr>
<tr><td colspan="3">2. Ранцевая криптографическая система. Основная идея. Алгоритм. Криптоанализ. (ОК 01, ОК 5, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6)</td></tr>
<tr><td colspan="3">3. Понятие хеш-функции. Основные требования, предъявляемые к криптографическим хеш-функциям. (ОК 01, ОК 02, ОК 03, ОК 04, ОК 5, ОК 06, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6)</td></tr>
</table>

3. Тестовые задания. Оценка по результатам тестирования.
3.1. Примерные задания теста по ПМ 02.

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6

1. Происхождение термина «криптография»:

- от слова «тайнопись»;
- от слова «шифрование»;
- от термина «скремблирование»;
- от термина «кодирование»;

2. Метод надежной передачи информации по открытому каналу связи использует:
- криптографию;
- стеганографию;
- кодирование;
- скремблирование;

3. Для чего используется система Kerberos?
- для симметричной аутентификации;
- для несимметричной аутентификации;
- для выработки ЭЦП;
- для шифрования;

4. Что такое код обнаружения манипуляции с данными MDC?
- есть результат действия хэш-функции;
- циклический контрольный код сообщения;
- код четности;
- имитоприставка;

5. Наука об обеспечении секретности и / или аутентичности (подлинности) передаваемых сообщений:
- ЭЦП;
- криптография;
- криптоанализ;
- стеганография;

6. Замену символов с открытого текста, соответствующими символами алфавита криптотекста называют:
- простейшим шифром;
- блочным шифром;
- шифром подстановки;
- шифром замены;

7. Функции, для которых легко найти функцию прямого отображения и нельзя найти обратное называются:
- линейные функции;
- нелинейные функции;
- односторонние функции;
- функции преобразования;

8. Цель атаки на криптосистему:
- нарушение целостности передачи информации абоненту;
- вскрытие ключа шифрования;
- фальсификация сообщения;
- вскрытие передаваемых зашифрованных сообщений;

9. Криптосистемы с последовательным выполнением преобразований над элементами открытого текста называется:
- поточными шифрами;
- двоичными аддитивными шифрами;
- блочными шифрами;
- криптосистемами с ключом однократного применения;

10. Установление санкционированным получателем (приемником) того факта, что полученное сообщение послано санкционированным отправителем (передатчиком) называется:
- идентификацией;
- аутентификацией;
- авторизацией;
- контролем целостности информации;

Компетенции ОК 01, ОК 5, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ОК 11, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6

1. Системы, где с помощью открытого ключа шифруют ключ блочного криптоалгоритма, а само сообщение шифруют с помощью этого симметричного секретного ключа, называют:
- гибридные криптосистемы;
- криптосистема RSA;
- электронная подпись;
- криптографические протоколы;

2. Как называют в ГОСТе режим электронной кодовой книги (ECB):
- режим сцепления блоков шифротекста;
- режим простой замены;
- режим обратных связей по выбору;
- режим счетчика;

3. Процесс применения шифра защищаемой информации называют:
- дешифрованием;
- вскрытием шифра;
- простой заменой;
- шифрованием;

4. Как называют в криптографии сменный элемент шифра, который применяется для шифрования конкретного сообщения:
- ключ;
- разрядность блока;
- число раундов шифрования;
- алгоритм шифрования;

5. Процесс наложения по определенному закону гамма-шифра на открытые данные:
- хэширование;
- имитовставка;
- гаммирование;
- ЭЦП;

6. Шифр – это …
- ключевое запоминающее устройство;
- совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с использованием ключей;
- состояние, выражающее процесс образования зашифрованных данных из открытых данных;
- значение исходных открытых параметров алгоритма криптографического преобразования;

7. Разрядность 3DES равна:
- 56 бит;
- 112 бит;
- 168 бит;
- 256 бит;

8. В чем состоит задача криптографа?
- взломать систему защиты
- обеспечить конфиденциальность и аутентификацию передаваемых сообщений

9. Верификация – это
- это проверка принадлежности субъекту доступа предъявленного им идентификатора.
- проверка целостности и подлинности инф, программы, документа
- это присвоение имени субъекту или объекту

10. Кодирование информации – это
- представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д.
- метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом

Компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 5, ОК 06, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6

1. При использовании классических криптографических алгоритмов ключ шифрования и ключ дешифрования совпадают и такие криптосистемы называются:
- простыми криптосистемами;
- гибридными криптосистемами;
- ассиметричными криптосистемами;
- симметричными криптосистемами;

2. Линейное шифрование данных , основанное на поточном способе шифрования называется:
- гаммированием;
- подстановкой;
- перестановкой;
- имитовставкой;

3. Криптографическая система открытого ключа, обеспечивающая такие механизмы защиты как шифрование и цифровая подпись, разработанная в 1977 году, называется:
- алгоритм шифрования RSA;
- алгоритм DSA;
- алгоритм DSS;
- алгоритм SHA;

4. Цифровая подпись - …
- подпись, которая ставится на документах;
- небольшое количество дополнительной цифровой информации, передаваемое вместе с подписываемым текстом, по которому можно удостоверится в аутентичности документа;
- код с исправлением ошибок;
- имитоприставка;

5. Функция, предназначенная для сжатия подписываемого документа до нескольких десятков, или сотен бит называется:
- логарифмической функцией;
- тригонометрической функцией;
- хэш- функцией;
- ЭЦП;

6. Этот алгоритм был разработан НИСТ и АНБ США в рамках стандарта безопасного хэширования SHS в 1992 году и предназначен для использования совместно с алгоритмом цифровой подписи DSA:
- DES;
- ГОСТ;
- Rundjael;
- SHA;

7. Чему равна разрядность блока алгоритма шифрования DES:
- 56 битам;
- 128 битам;
- 64 битам;
- 256 битам;

8. Последовательность случайных чисел должна быть
- монотонно возрастающей
- монотонно убывающей
- иметь равномерное распределение

9. В DSS используется следующая хэш-функция
- MD5
- SHA-1
- SHA-2

10. Алгоритм MARS обладает следующими свойствами
- имеет самое быстрое установление ключа
- имеет самое быстрое шифрование/дешифрование
- имеет возможность вычисления подключей на лету
- шифрование и дешифрование имеют идентичные функции

3.2. Соответствие между бальной системой и системой оценивания по результатам тестирования устанавливается посредством следующей таблицы:

Объект оценки	Показатели оценивания результатов обучения	Оценка	Уровень результатов обучения
Обучающийся	60 баллов и менее	«Неудовлетворительно»	Низкий уровень
	74 – 61 баллов	«Удовлетворительно»	Пороговый уровень
	84 – 75 баллов	«Хорошо»	Повышенный уровень
	100 – 85 баллов	«Отлично»	Высокий уровень

4. Оценка ответа обучающегося на вопросы экзаменационного билета.

4.1. Оценка ответа обучающегося на вопросы экзаменационного билета.

Элементы оценивания	Содержание шкалы оценивания			
	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
Соответствие ответов формулировкам вопросов (заданий)	Полное несоответствие по всем вопросам	Значительные погрешности	Незначительные погрешности	Полное соответствие

Структура, последовательность и логика ответа. Умение четко, понятно, грамотно и свободно излагать свои мысли	Полное несоответствие критерию.	Значительное несоответствие критерию	Незначительное несоответствие критерию	Соответствие критерию при ответе на все вопросы.
Знание нормативных, правовых документов и специальной литературы	Полное незнание нормативной и правовой базы и специальной литературы	Имеют место существенные упущения (незнание большей части из документов и специальной литературы по названию, содержанию и т.д.).	Имеют место несущественные упущения и незнание отдельных (единичных) работ из числа обязательной литературы.	Полное соответствие данному критерию ответов на все вопросы.
Умение увязывать теорию с практикой, в том числе в области профессиональной работы	Умение связать теорию с практикой работы не проявляется.	Умение связать вопросы теории и практики проявляется редко.	Умение связать вопросы теории и практики в основном проявляется.	Полное соответствие данному критерию. Способность интегрировать знания и привлекать сведения из различных научных сфер
Качество ответов на дополнительные вопросы	На все дополнительные вопросы преподавателя даны неверные ответы.	Ответы на большую часть дополнительных вопросов преподавателя даны неверно.	1. Даны неполные ответы на дополнительные вопросы преподавателя. 2. Дан один неверный ответ на дополнительные вопросы преподавателя.	Даны верные ответы на все дополнительные вопросы преподавателя.

Примечание: итоговая оценка формируется как средняя арифметическая результатов элементов оценивания.