Министерство науки и высшего образования РФ
Образовательная автономная некоммерческая организация
высшего образования
«Волжский университет имени В.Н. Татищева» (институт)

УТВЕРЖДАЮ
Ректор Якушин В.А.
от 02.05.2023г. № 77/1

Рабочая программа

Защита информации

Направление подготовки 09.03.02 Информационные системы и технологии

Квалификация (степень) выпускника – бакалавр

Форма обучения – очная, заочная, очно-заочная

Тольятти, 2023 г.

Рабочая программа **Защита информации** составлена с требованиями ФГОС, ВО, ОПОП по направлению подготовки 09.03.02 Информационные системы и технологии (уровень высшего образования: бакалавриат) и учебного плана.

Программа обсуждена и рекомендована к использованию и (или) изданию решением кафедры на заседании кафедры «Информатика и системы управления»
протокол № 09 от 19.04.2023г.
Зав. кафедрой ИиСУ
к.п.н., доцент Е.Н. Горбачевская

Одобрено Учебно-методическим советом вуза
протокол № 4/23 от 27.04.2023г
Председатель УМС
к.п.н. И.И. Муртаева

1. ПЕРЕЧЕНЬ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

В результате освоения дисциплины у обучающихся должны быть сформированы следующие общепрофессиональные компетенции и профессиональные компетенции:

Наименование компетенции	Код компетенции
Способен выполнять работы по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	ПК-1

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Данная учебная дисциплина относится к к части, формируемой участниками образовательных отношений 09.03.02 «Информационные системы и технологии».

В таблице 1 представлен перечень компетенций с указанием перечня дисциплин, формирующих эти компетенции согласно учебному плану ОПОП

Таблица 1

Код компетенции	Наименование компетенции, формируемой в рамках освоения дисциплины	Предшествующие дисциплины, формирующие указанную компетенцию	Последующие дисциплины, формирующие указанную компетенцию
ПК-1	Способен выполнять работы по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	Моделирование Системное программное обеспечение Базовые технологии и процессы Сети и телекоммуникации Надежность систем Электронный бизнес Методы и средства проектирование информационных систем и технологий	Научно исследовательская работа Инструментальные средства информационных систем Архитектура информационных систем Производственная практика. Технологическая (проектно-технологическая) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

* в качестве этапа формирования компетенций используются номера семестров согласно учебного плана ОПОП

Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы направления подготовки, представлен в таблице:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ПК-1 Способен выполнять работы по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	ПК-1.1. Планирует процедуры создания, сопровождения и интеграции программных модулей и компонент ИС, автоматизирующих задачи организационного управления и бизнес-процессы ПК 1.2. Разрабатывает, сопровождает и интегрирует программные модули и компоненты ИС, автоматизирующих задачи организационного управления и бизнес-процессы ПК 1.4. Организует интеграцию программных модулей и компонент и верификацию программного продукта

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Вид учебной работы	**Всего**	**Семестр**
		7
Общая трудоёмкость дисциплины	144 час 4 з.е.	144 час 4 з.е.
Контактная работа с преподавателем (всего)	64	64
В том числе:		
Лекции	32	32
Практические / семинарские занятия	-	-
Лабораторные занятия	32	32
Консультации	-	-
Самостоятельная работа (всего)	44	44
В том числе (если есть):		
Курсовой проект / работа	-	-
Расчетно-графическая работа	-	-
Контрольная работа	-	-
Реферат / эссе / доклад	-	-
Иное	*44*	*44*
Вид промежуточной аттестации (зачет, экзамен)	Экзамен (36)	Экзамен (36)

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Вид учебной работы	**Всего**	**Семестр**
		7
Общая трудоёмкость дисциплины	144 час 4 з.е.	144 час 4 з.е.
Контактная работа с преподавателем (всего)	16	16
В том числе:		
Лекции	8	8
Практические / семинарские занятия	-	-
Лабораторные занятия	8	8
Консультации	-	-
Самостоятельная работа (всего)	92	92
В том числе (если есть):		
Курсовой проект / работа	-	-
Расчетно-графическая работа	-	-
Контрольная работа	-	-
Реферат / эссе / доклад	-	-
Иное	*92*	*92*
Вид промежуточной аттестации (зачет, экзамен)	Экзамен(36)	Экзамен(36)

ОЧНО-ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Вид учебной работы	Всего	Семестр
		7
Общая трудоёмкость дисциплины	144 час 4 з.е.	144 час 4 з.е.
Контактная работа с преподавателем (всего)	22	22
В том числе:		
Лекции	16	16
Практические / семинарские занятия	-	-
Лабораторные занятия	16	16
Консультации	-	-
Самостоятельная работа (всего)	76	76
В том числе (если есть):		
Курсовой проект / работа	-	-
Расчетно-графическая работа	-	-
Контрольная работа	-	-
Реферат / эссе / доклад	-	-
Иное	*76*	*76*
Вид промежуточной аттестации (зачет, экзамен)	Экзамен(36)	Экзамен(36)

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. КАЛЕНДАРНО-ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

№ п/п	Тема	Количество часов на			
		лекции	практические /семинарские занятия	лабораторные занятия	самостоятельную работу
1	Тема 1. Основные понятия и определения предмета защиты информации	2			3
2	Тема 2. Разграничение доступа к ресурсам	2			3
3	Тема 3. Идентификация и аутентификация субъектов	2			3
4	Тема 4. Методы и средства криптографической защиты	2			3
5	Тема 5. Контроль целостности информации. Электронно-цифровая подпись	2			3
6	Тема 6. Хранение и распределение ключевой информации. Протоколы	2			3

	безопасной аутентификации пользователей				
7	Тема 7. Защита программного обеспечения от несанкционированного использования	4			3
8	Тема 8. Защита от разрушающих программных воздействий	4			3
9	Тема 9. Защита информации в компьютерных сетях	4		32	11
10	Тема 10. Инженерно-техническая защита информации	4			3
11	Тема 11. Руководящие документы России. Правовое обеспечение информационной безопасности и противодействию терроризму.	4			3
Итого		32		32	44

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

№ п/п	Тема	Количество часов на			
		лекции	практические /семинарские занятия	лабораторные занятия	самостоятельную работу
1	Тема 1. Основные понятия и определения предмета защиты информации	0.5			9
2	Тема 2. Разграничение доступа к ресурсам	0.5			9
3	Тема 3. Идентификация и аутентификация субъектов	0.5			9
4	Тема 4. Методы и средства криптографической защиты	0.5			9
5	Тема 5. Контроль целостности информации. Электронно-цифровая подпись	1			9
6	Тема 6. Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей	1			8
7	Тема 7. Защита программного обеспечения от несанкционированного использования	1			8
8	Тема 8. Защита от разрушающих программных	1			8

	воздействий				
9	Тема 9. Защита информации в компьютерных сетях	1		8	8
10	Тема 10. Инженерно-техническая защита информации	1			8
11	Тема 11. Руководящие документы России. Правовое обеспечение информационной безопасности и противодействию терроризму.	1			8
Итого		8		8	92

ОЧНО-ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

№ п/п	Тема	Количество часов на			
		лекции	практические /семинарские занятия	лабораторные занятия	самостоятельную работу
1	Тема 1. Основные понятия и определения предмета защиты информации	1			7
2	Тема 2. Разграничение доступа к ресурсам	1			7
3	Тема 3. Идентификация и аутентификация субъектов	1			7
4	Тема 4. Методы и средства криптографической защиты	1			7
5	Тема 5. Контроль целостности информации. Электронно-цифровая подпись	2			7
6	Тема 6. Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей	2			7
7	Тема 7. Защита программного обеспечения от несанкционированного использования	2			8
8	Тема 8. Защита от разрушающих программных воздействий	2			7
9	Тема 9. Защита информации в компьютерных сетях	2		16	7
10	Тема 10. Инженерно-техническая защита информации	2			7
11	Тема 11. Руководящие документы России. Правовое	2			6

	обеспечение информационной безопасности и противодействию терроризму.				
Итого		16		16	76

4.2. КРАТКОЕ СОДЕРЖАНИЕ ЛЕКЦИОННОГО КУРСА

Тема 1. Основные понятия и определения предмета защиты информации
Санкционированный и несанкционированный доступ. Базовые свойства безопасности информации. Угрозы безопасности и каналы реализации угроз. Основные принципы обеспечения информационной безопасности. Ценность информации. Меры обеспечения безопасности компьютерных систем. Характеристика способов защиты компьютерной информации с помощью аппаратно-программных мер.

Тема 2. Разграничение доступа к ресурсам
Политики безопасности. Классификация политик безопасности. Политики избирательного разграничения доступа. Мандатные политики безопасности. Контроль доступа, базирующийся на ролях. Политики безопасности контроля целостности информационных ресурсов.

Тема 3. Идентификация и аутентификация субъектов
Классификация подсистем идентификации и аутентификации субъектов. Парольные системы идентификации и аутентификации пользователей. Идентификация и аутентификация пользователей с использованием технических устройств. Идентификация и аутентификация с использованием индивидуальных биометрических характеристик пользователя.

Тема 4. Методы и средства криптографической защиты
Принципы криптографической защиты информации. Традиционные симметричные криптосистемы: шифрование методом замены, шифрование методами перестановки, шифрование методом гаммирования. Элементы криптоанализа. Современные симметричные системы шифрования: стандарт шифрования DES (США), отечественный стандарт симметричного шифрования. Асимметричные криптосистемы: недостатки симметричных криптосистем и принципы асимметричного шифрования, однонаправленные функции, алгоритм шифрования RSA,

Тема 5. Контроль целостности информации. Электронно-цифровая подпись
Проблема обеспечения целостности информации. Функции хэширования и электронно-цифровая подпись. Инфраструктура открытых ключей PKI.

Тема 6. Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей
Типовые схемы хранения ключевой информации. Защита баз данных аутентификации в ОС Windows и UNIX. Иерархия ключевой информации. Распределение ключей. Протоколы безопасной удаленной аутентификации пользователей.

Тема 7. Защита программного обеспечения от несанкционированного использования
Проблема защиты программного обеспечения от несанкционированного использования. Модульная архитектура технических средств защиты ПО от несанкционированного использования. Функционирование подсистем и модулей системы защиты ПО от

несанкционированного использования. Электронные ключи HASP. Защита ПО от изучения: базовые методы нейтрализации систем защиты от несанкционированного использования, понятие и средства обратного проектирования, локализация кода модуля защиты посредством отлова WinAPI функций в режиме отладки, базовые методы противодействия отладчикам, базовые методы противодействия дизассемблированию ПО, защита от отладки, основанная на особенностях конвейеризации процессора, использование недокументированных инструкций и недокументированных возможностей процессора, шифрование кода программы как универсальный метод противодействия отладке и дизассемблированию.

Тема 8. Защита от разрушающих программных воздействий
Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и РПВ. Компьютерные вирусы как класс РПВ. Защита от РПВ. Изолированная программная среда.

Тема 9. Защита информации в компьютерных сетях
Основные угрозы и причины уязвимости сети INTERNET. Классификация типовых удаленных атак на интрасети. Подходы к защите от типовых удаленных атак. Ограничение доступа в сеть. Межсетевые экраны. Виртуальные частные сети (VPN). Доменная архитектура в Windows NT. Служба Active Directory. Централизованный контроль удаленного доступа. Серверы аутентификации.

Тема 10. Инженерно-техническая защита информации
Радиомикрофоны. Устройства перехвата телефонных сообщений. Специализированные устройства. Обнаружение, локализация и подавление закладных подслушивающих устройств. Предотвращение утечки информации через побочные электромагнитные излучения и наводки.

Тема 11. Руководящие документы России. Правовое обеспечение информационной безопасности и противодействию терроризму.
Показатели защищенности средств вычислительной техники от НСД. Статья 272 УК РФ. Статья 273 УК РФ. Статья 274 УК РФ. Статья 146. Нарушение авторских и смежных прав. Статья 147. Нарушение изобретательских и патентных прав. Законодательное противодействие распространению террористических материалов в Интернет. Проблемы экспертизы информационных материалов, содержащих признаки идеологии терроризма.

4.3. ТЕМАТИКА ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Лабораторная работа № 1 Базовые механизмы безопасности коммутаторов
Лабораторная работа № 2 Безопасность на основе сегментации трафика
Лабораторная работа № 3 Безопасность на основе протокола IEEE 802.1x
Лабораторная работа № 4 Списки контроля доступа ACL
Лабораторная работа № 5 Утилита iptables
Лабораторная работа № 6 Туннелирование соединений с использованием протокола SSL
Лабораторная работа № 7 Удаленное управление по защищенному протоколу SSH
Лабораторная работа № 8 Протокол PPPoE

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

5.1 Основная литература

Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее

образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490019

Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497002

5.2 Дополнительная литература

Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490277

Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2022. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489242

5.3. Ресурсы информационно-коммуникационной сети «Интернет»

Адрес Интернет ресурса	Название Интернет ресурса	Режим доступа
http://intuit.ru/	Интернет-университет информационных технологий	Свободный
http://vkit.ru/	Сайт журнала «Вестник компьютерных и информационных технологий»	Свободный
http://ru.wikipedia.org/.	Свободная общедоступная мультиязычная универсальная интернет-энциклопедия	Свободный

6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

Дисциплина «**Защита информации**» изучается в течение одного семестра. При планировании и организации времени, необходимого на изучение обучающимся дисциплины, необходимо придерживаться следующих рекомендаций.

В период между сессиями студенты должны вести конспект лекций, изучать теоретический материал в соответствии с программой курса, выполнять предложенные преподавателем задания для самостоятельной работы, готовиться к сдаче зачета и экзамена, прорабатывая необходимый материал согласно перечню вопросов для подготовки к зачету и экзамену и списку рекомендованной литературы.

Выполнение лабораторных работ относится к числу обязательных видов работ. Перед выполнением работы необходимо внимательно ознакомиться с теоретическим материалом, представленным в методических указаниях к соответствующей лабораторной работе. При необходимости можно воспользоваться рекомендуемой литературой. В ходе выполнения работы необходимо руководствоваться порядком выполнения лабораторной работы и указаниями преподавателя, при этом должны соблюдаться правила техники безопасности. Результатом выполнения работы является отчёт, который должен быть аккуратно оформлен и выполнен в соответствии с требованиями, приведенными в методических указаниях.

В указанное преподавателем время обучающиеся защищают отчеты. Защита проводится в виде собеседования по контрольным вопросам, приведенным в методических

указаниях. Кроме того, преподаватель может задавать дополнительные вопросы, касающиеся результатов эксперимента, выводов по результатам опытов и т.п. К промежуточной аттестации допускаются обучающиеся, выполнившие все лабораторные работы и защитившие отчеты по ним. При наличии задолженности по лабораторным работам, по согласованию с преподавателем, возможна замена работы по выполнению отчета на реферат по теме соответствующего лабораторного занятия с последующей его защитой.

В течение семестра и во время сессии основным видом подготовки являются самостоятельные занятия. Они включают в себя изучение вопросов, вынесенных на самостоятельное изучение, оформление отчетов по лабораторным работам, курсовое проектирование, а так же подготовку к промежуточной аттестации

Систематическая работа в соответствии с программой дисциплины – условие успешного освоения материала.

Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ограниченными возможностями здоровья.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Медиаматериалы также следует использовать и адаптировать с учетом индивидуальных особенностей обучения лиц с ОВЗ.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);
- в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);
- методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);
- выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);

- устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

7. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

При проведение занятий по дисциплине используются следующие программные продукты:

1. Linux (свободное ПО)
2. Windows (для академических организациях, лицензия Microsoft Imagine (ранее MSDN AA, Dream Spark);
3. FileZilla FTP Client (свободное многоязычный FTP – клиент с открытым исходным кодом);
4. Google Chrome (свободное ПО);
5. Программа NetCracker Professional предназначенная для проектирования и моделирования компьютерных сетей;
6. Cisco Packet Tracer 5.1 - последняя версия программы комплексной сетевой технологии преподавания и обучения Cisco Networking Academy.

8. НЕОБХОДИМАЯ МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

Оборудование лекционных аудиторий Б-604: офисная мебель на 20 мест, демонстрационное оборудование: экран – 1 шт.; проектор – 1 шт.; 9 ПК с доступом в Интернет и ЭИОС. Оборудование аудиторий для лабораторных занятий: ауд. Б-604: офисная мебель на 20 мест, демонстрационное оборудование: экран – 1 шт.; проектор – 1 шт.; 9 ПК с доступом в Интернет и ЭИОС;

Учебно-лабораторный комплекс «Корпоративные компьютерные сети» (ЮУрГУ-НПИ «Учебная техника и технологии», Челябинск, 2011, №5)

Комплект коммутационного оборудования D-Link.

Оборудование аудиторий для самостоятельной работы: читальный зал НТБ: 5 ПК с доступом в Интернет; ауд. Б-609: офисная мебель на 20 мест, 9 ПК с доступом в Интернет и ЭИОС, демонстрационное оборудование: проектор – 1 шт.; экран, доска ученическая, рабочее место преподавателя.

Разработчик:

Кафедра ИиСУ	**к.т.н., доцент**	**Н.О.Куралесова**
(место работы)	*(занимаемая должность)*	*(инициалы, фамилия)*

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ОБРАЗОВАТЕЛЬНАЯ АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОЛЖСКИЙ УНИВЕРСИТЕТ имени В.Н. ТАТИЩЕВА» (институт)

.

Фонд оценочных средств

«Защита информации»

для направления подготовки

09.03.02 «Информационные системы и технологии»

Квалификация (степень) выпускника – бакалавриат

Тольятти 2023

1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Оценочные средства разработаны для оценки профессиональных компетенций: ПК-2.

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты освоения основной профессиональной образовательной программы (ОПОП) – компетенции обучающихся определяются требованиями стандарта по направлению подготовки (специальности) и формируются в соответствии с матрицей компетенций ОПОП (Таблица 2)

Планируемые результаты обучения по дисциплине – знания, умения, навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций и обеспечивающие достижение планируемых результатов освоения образовательной программы, формируются в соответствии с картами компетенций ОПОП.

Таблица 1

Планируемые результаты обучения по дисциплине

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ПК-1 Способен выполнять работы по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	ПК-1.1. Планирует процедуры создания, сопровождения и интеграции программных модулей и компонент ИС, автоматизирующих задачи организационного управления и бизнес-процессы ПК 1.2. Разрабатывает, сопровождает и интегрирует программные модули и компоненты ИС, автоматизирующих задачи организационного управления и бизнес-процессы ПК 1.4. Организует интеграцию программных модулей и компонент и верификацию программного продукта

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

Результаты обучения по дисциплине «Защита информации» направления подготовки 09.03.02 «Информационные системы и технологии» определяются показателями и критериями оценивания сформированности компетенций на этапах их формирования представлены в табл. 2.

Таблица 2

Матрица соответствия оценочных средств запланированным результатам обучения

Компетенции	Оценочные средства		
	Текущий контроль		Промежуточный контроль
	Оценочное средство 1 (лабораторное задания)		Экзамен
ПК-1	ПК-1.1. ПК -1.2. ПК -1.4.		ПК-1.1. ПК -1.2. ПК -1.4.

Показатели и критерии оценивания сформированности компетенций (промежуточного контроля)

На этапе промежуточной аттестации используется система оценки успеваемости обучающихся, которая позволяет преподавателю оценить уровень освоения материала обучающимися. Критерии оценивания сформированности планируемых результатов обучения (дескрипторов) представлены в карте компетенции ОПОП.

Форма оценки знаний: оценка - 5 «отлично»; 4 «хорошо»; 3 «удовлетворительно»; 2 «неудовлетворительно». Лабораторные работы, практические занятия, практика оцениваются: «зачет», «незачет». Возможно использование балльно-рейтинговой оценки.

Шкала оценивания:

«Зачет» – выставляется, если сформированность заявленных дескрипторов компетенций на *_51_%* и более оценивается не ниже «удовлетворительно» при условии отсутствия критерия «неудовлетворительно». Выставляется, когда обучающийся показывает хорошие знания изученного учебного материала; самостоятельно, логично и последовательно излагает и интерпретирует материалы учебного курса; полностью раскрывает смысл предлагаемого вопроса; владеет основными терминами и понятиями изученного курса; показывает умение переложить теоретические знания на предполагаемый практический опыт.

«Отлично» – выставляется, если сформированность заявленных дескрипторов компетенций __85__*%* более (в соответствии с картами компетенций ОПОП) оценивается критериями «хорошо» и «отлично», при условии отсутствия оценки «неудовлетворительно»: студент показал прочные знания основных положений фактического материала, умение самостоятельно решать конкретные практические задачи повышенной сложности, свободно использовать справочную литературу, делать обоснованные выводы из результатов анализа конкретных ситуаций;

«Хорошо» – выставляется, если сформированность заявленных дескрипторов компетенций на *_61__%* и более (в соответствии с картами компетенций ОПОП) оценивается критериями «хорошо» и «отлично», при условии отсутствия оценки «неудовлетворительно», допускается оценка «удовлетворительно»: обучающийся показал прочные знания основных положений фактического материала, умение самостоятельно решать конкретные практические задачи, предусмотренные рабочей программой, ориентироваться в рекомендованной справочной литературе, умеет правильно оценить полученные результаты анализа конкретных ситуаций;

«Удовлетворительно» – выставляется, если сформированность заявленных дескрипторов компетенций *__51_%* и более (в соответствии с картами компетенций ОПОП) оценивается критериями «удовлетворительно», «хорошо» и «отлично»: обучающийся показал знание основных положений фактического материала, умение получить с помощью преподавателя правильное решение конкретной практической задачи из числа предусмотренных рабочей программой, знакомство с рекомендованной справочной литературой;

«Неудовлетворительно» «Незачет» – выставляется, если сформированность заявленных дескрипторов компетенций менее чем *_51_%* (в соответствии с картами компетенций ОПОП): при ответе обучающегося выявились существенные пробелы в знаниях основных положений фактического материала, неумение с помощью преподавателя получить правильное решение конкретной практической задачи из числа предусмотренных рабочей программой учебной дисциплины.

Ответы и решения обучающихся оцениваются по следующим общим критериям: распознавание проблем; определение значимой информации; анализ проблем; аргументированность; использование стратегий; творческий подход; выводы; общая грамотность.

Соответствие критериев оценивания сформированности планируемых результатов обучения (дескрипторов) системам оценок представлено в табл.

Таблица 4

Интегральная оценка

Критерии	Традиционная оценка	Балльно-рейтинговая оценка
5	5	86 - 100
4	4	61-85
3	3	51-60
2 и 1	2, Незачет	0-50
5, 4, 3	Зачет	51-100

Обучающиеся обязаны сдавать все задания в сроки, установленные преподавателем. Оценка «Удовлетворительно» по дисциплине, может выставляться и при неполной сформированности компетенций в ходе освоения отдельной учебной дисциплины, если их формирование предполагается продолжить на более поздних этапах обучения, в ходе изучения других учебных дисциплин.

Показатели и критерии оценки достижений студентом запланированных результатов освоения
дисциплины в ходе текущего контроля и промежуточной аттестации

Оценка, уровень	**Критерии**
«отлично», повышенный уровень	Студент показал прочные знания основных положений фактического материала, умение самостоятельно решать конкретные практические задачи повышенной сложности, свободно использовать справочную литературу, делать обоснованные выводы из результатов анализа конкретных ситуаций
«хорошо», пороговый уровень	Студент показал прочные знания основных положений фактического материала, умение самостоятельно решать конкретные практические задачи, предусмотренные рабочей программой, ориентироваться в рекомендованной справочной литературе, умеет правильно оценить полученные результаты анализа конкретных ситуаций
«удовлетворительно», пороговый уровень	Студент показал знание основных положений фактического материала, умение получить с помощью преподавателя правильное решение конкретной практической задачи из числа предусмотренных рабочей программой, знакомство с рекомендованной справочной литературой
«неудовлетворительно», уровень не сформирован	При ответе студента выявились существенные пробелы в знаниях основных положений фактического материала, неумение с помощью преподавателя получить правильное решение конкретной практической задачи из числа предусмотренных рабочей программой учебной дисциплины

3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

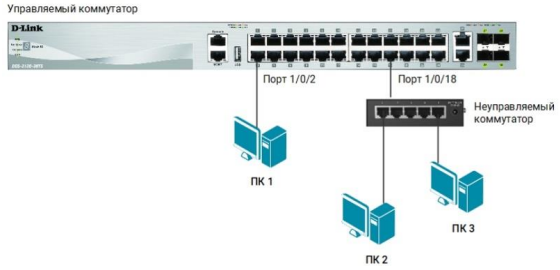
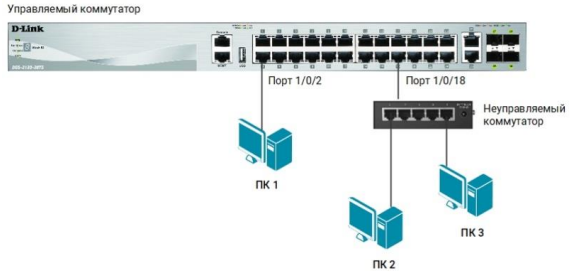
Перечень компетенций и индикаторов достижения компетенций, для оценки сформированности которых используется данный ФОС

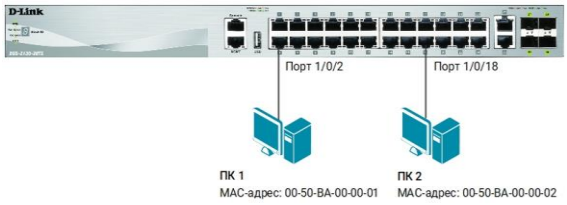
Код и наименование компетенции	**Код и наименование индикатора достижения компетенции, реализуемые дисциплиной**

ПК-1 Способен выполнять работы по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	ПК-1.1. Планирует процедуры создания, сопровождения и интеграции программных модулей и компонент ИС, автоматизирующих задачи организационного управления и бизнес-процессы ПК 1.2. Разрабатывает, сопровождает и интегрирует программные модули и компоненты ИС, автоматизирующих задачи организационного управления и бизнес-процессы ПК 1.4. Организует интеграцию программных модулей и компонент и верификацию программного продукта

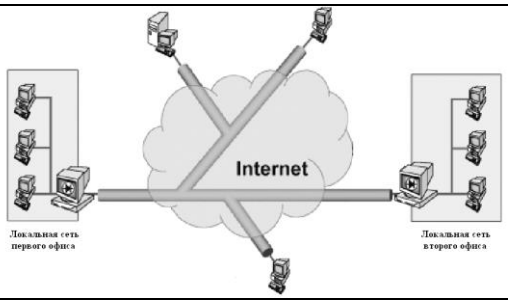
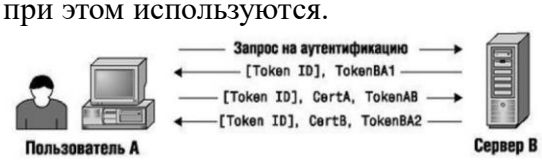
Номер задания	Содержание вопроса	Правильный ответ на задание
1.	Выберите правильный вариант ответа Одним из основных принципов обеспечения информационной безопасности в информационно-коммуникационных средах являются _____ который предполагает необходимость учета всех слабых и уязвимых мест АСОИ, возможных объектов и направлений атак, высокую квалификацию злоумышленника, текущих и возможных в будущем каналов реализации угроз. A) принцип разумной достаточности B) принцип непрерывности защиты C) принцип комплексности **D) принцип системности**	D
2.	Выберите правильный вариант ответа Одним из основных принципов обеспечения информационной безопасности в информационно-коммуникационных средах являются _____ который предполагает возможность варьировать уровень ее защищенности A) принцип системности B) принцип комплексности C) принцип непрерывности защиты **D) принцип гибкости управления и применения системы защиты**	D
3.	Выберите правильный вариант ответа. Анализ сетевого трафика в информационно-коммуникационных средах осуществляется путем его перехвата является внутрисегментной атакой и направлен на перехват и анализ информации, предназначенной для любого ПК, расположенного в том же сегменте сети, что и злоумышленник и называется A) DoS атаками (DoS – Denied of Service) B) Маскарад (spoofing) **C) Сниффинг (sniffing)**	C

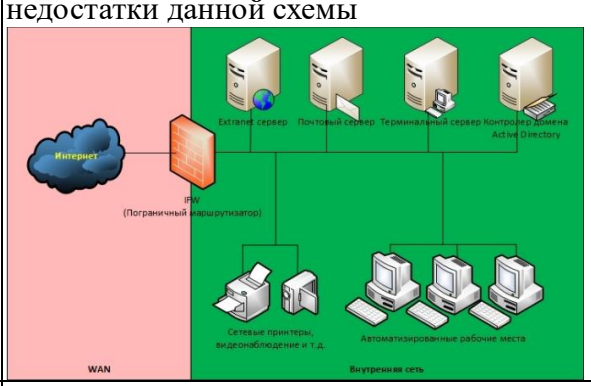
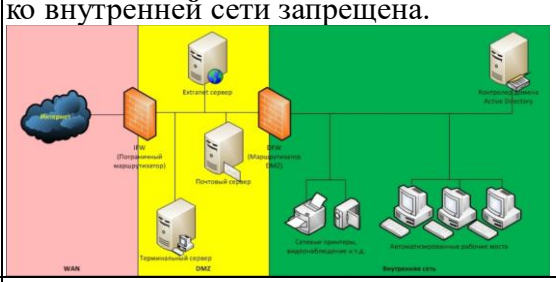
Номер задания	Содержание вопроса	Правильный ответ на задание
	D) Фишинг (fishing)	
4.	Выберите правильный вариант ответа. При организации безопасности доступа в информационно-коммуникационных средах межсетевые экраны осуществляют фильтрацию входящих в сеть и исходящих из сети пакетов на основе информации, содержащихся в их TCP и IP заголовках, называются **A) фильтрующие маршрутизаторы** B) шлюзы сетевого уровня C) шлюзы прикладного уровня D) маршрутизаторы защиты	A
5.	Выберите правильный вариант ответа. Поставленная задача: Настроить функцию Port Security коммутатора серии DES-3810 на режим запоминания MAC-адресов; по умолчанию все порты находятся в режиме continuous. Выберите параметр настройки **A) learn-mode** B) mac-address C) action D) address-limit F) clear-intrusion-flag	A
6.	Выберите правильный вариант ответа. Поставленная задача: Настроить функцию Port Security коммутатора серии DES-3810 на статическое задание разрешенных MAC-адресов для режимов static и configured A) learn-mode **B) mac-address** C) action D) address-limit F) clear-intrusion-flag	B
7.	Выберите правильный вариант ответа. Поставленная задача: Настроить функцию Port Security коммутатора серии DES-3810 на максимальное количество MAC-адресов, которое будет разрешено на порту A) learn-mode B) mac-address C) action **D) address-limit** F) clear-intrusion-flag	D
8.	Выберите правильный вариант ответа. Поставленная задача: Дана схема сети (рисунок). Опишите действия внесенных настроек	A

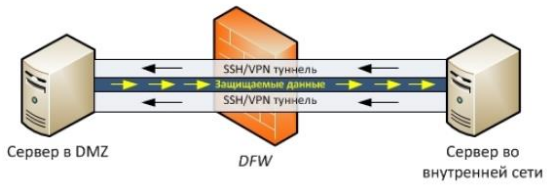
Номер задания	Содержание вопроса	Правильный ответ на задание
	 Switch# configure terminal Switch(config)#interface range ethernet 1/0/1-24 Switch(config-if-range)#switchport port-security Switch(config-if-range)#switchport port-security maximum 1 **A) включена на портах 1/0/1-24 функция Port Security и установлено максимальное количество изучаемых каждым портом MAC-адресов равное 1** B) установлен режим работы фунции Delete on Timeout C) указано действие при превышении максимального числа MAC-адресов — ограничение (Restrict) D) настроено время жизни для динамически изученных MAC-адресов равное 3 минутам	
9.	Выберите правильный вариант ответа. Поставленная задача: Дана схема сети (рисунок). Опишите действия внесенных настроек  Switch(config-if-range)# switchport port-security aging time 3 A) включена на портах 1/0/1-24 функция Port Security и установлено максимальное количество изучаемых каждым портом MAC-адресов равное 1 B) установлен режим работы фунции	D

Номер задания	Содержание вопроса	Правильный ответ на задание
	Delete on Timeout C) указано действие при превышении максимального числа MAC-адресов — ограничение (Restrict) **D) настроено время жизни для динамически изученных MAC-адресов равное 3 минутам**	
10.	Выберите правильный вариант ответа. Поставленная задача: Дана схема сети (рисунок). Опишите действия внесенных настроек  Switch(config)#mac-address-table static 0050.BA00.0001 vlan 1 interface ethernet 1/0/2 Switch(config)#mac-address-table static 0050.BA00.0002 vlan 1 interface ethernet 1/0/18 A) включена на портах 1/0/1-24 функция Port Security и установлено максимальное количество изучаемых каждым портом MAC-адресов равное 1 **B) созданы статические записи для MAC-адресов рабочих станций, подключённых к портам 1/0/2 и 1/0/18** C) указано действие при превышении максимального числа MAC-адресов — ограничение (Restrict) D) настроено время жизни для динамически изученных MAC-адресов равное 3 минутам	B
11.	Выберите правильный вариант ответа. На рисунке показана схема _____  **A) DDoS атаками (Distributed Denial of Service)**	A

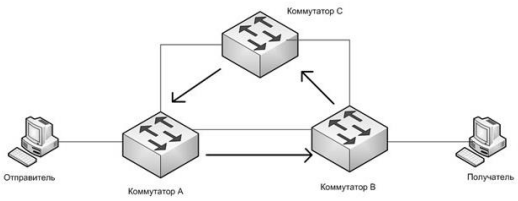
Номер задания	Содержание вопроса	Правильный ответ на задание
	B) Маскарад (spoofing) C) Сниффинг (sniffing) D) Фишинг (fishing)	
12.	Выберите правильный вариант ответа. Высшую степень защиты обеспечивает метод шифрования информации _____. A) хеширование **B) гаммирование** C) закрытых ключей D) профилей пользователей	B
13.	Выберите правильный вариант ответа. Active Directory использует протокол **A) LDAP (Lightweight Directory Access Protocol)** B) ICMP (Internet Control Message Protocol) C) SNMP (Simple Network Management Protocol) D) RAMUS	A
14.	Выберите правильный вариант ответа. Протокол для реализации аутентификации, авторизации и сбора сведений об использованных ресурсах, разработанный для передачи сведений между центральной платформой и оборудованием. A) UDP (User Datagram Protocol) B) SNMP (Simple Network Management Protocol) C) RSVP (Resource ReSerVation Protocol) **D) RADIUS (Remote Authentication in Dial-In User Service)**	D
15.	Выберите правильный вариант ответа. Криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле. Криптосистема включает в себя алгоритм шифрования и алгоритм цифровой подписи. **A) Схема Эль-Гамаля** B) Протокол MTI/A(C) Протокол Диффи—Хеллмана D) Протокол Station-to-Station	A
16.	На рисунке представлена схема сети с обеспечением безопасной передачи данных. На основе какой технологии организованная безопасность в информационно-коммуникационной среде организации?	Безопасность в информационно-коммуникационной среде данной организации организованна на основе виртуальной частной сети.

Номер задания	Содержание вопроса	Правильный ответ на задание
		
17.	Укажите технологию организации безопасного доступа в информационно-коммуникационных системах при информационном скрытии речевой.	При организации безопасности доступа в информационно-коммуникационных системах информационное скрытие речевой информации обеспечивается техническим закрытием аналоговым скремблированием и шифрованием сигналов речевой информации, передаваемых по кабелям и радиоканалам.
18.	Опишите действие команды коммутатора серии DES-3810 функцию Port Security switch(config)# port-security 10 clear-intrusion-flag switch(config)# interface 10 enable	Включение порта 10 после того, как он был выключен Port Security, то есть после его блокировки
19.	Опишите действие команды коммутатора серии DES-3810 функцию Port Security switch(config)# aaa port-access authenticator 10 control auto	Настроена функия Port Security с аутентификацией 802.1X на порт 10. Режим контроля auto
20.	На рисунке показана схема аутентификации методом сертификатов. Приведите примеры протоколов которые при этом используются. 	Аутентификацию при помощи сертификатов обеспечивают несколько распространенных протоколов, в частности, наиболее известный и широко распространенный протокол SSL, который применяется практически в каждом web-браузере. Помимо него применяются протоколы TLS, IKE, S/MIME, PGP и Open PGP.
21.	Опишите для чего используется Протокол Диффи — Хеллмана (Diffie–Hellman key exchange protocol, DH).	Протокол Диффи — Хеллмана — криптографический протокол, позволяющий двум и более сторонам получить общий секретный ключ, используя незащищенный от прослушивания канал связи. Полученный ключ используется для шифрования дальнейшего обмена с помощью алгоритмов симметричного шифрования.

Номер задания	Содержание вопроса	Правильный ответ на задание
22.	Перечислите источники угроз в Ethernet.	Источник угроз делят на 2 типа: 1) источники угроз в самой системе; 2) источники угроз вне системы.
23.	На рисунке представлена схема плоской сети. Доступ узлов в Интернет осуществляется через NAT, а доступ к сервисам из Интернет через Port forwarding. Опишите достоинства т недостатки данной схемы 	Плюсы варианта предложенной схемы плоской сети: 1) Минимальные требования к функционалу IFW (можно сделать практически на любом, даже домашнем роутере). 2) Минимальные требования к знаниям специалиста, осуществляющего реализацию варианта. 3) Минусы варианта: 4) Минимальный уровень безопасности.
24.	На рисунке представлена схема сети с DMZ. Для увеличения информационной безопасности, данные доступные из Интернет, помещают в специально выделенный сегмент – демилитаризованную зону (DMZ). DMZ организуется с помощью межсетевых экранов, отделяющих ее от Интернет (IFW) и от внутренней сети (DFW). При этом правила фильтрации межсетевых экранов выглядят следующим образом: 1.Из внутренней сети можно инициировать соединения в DMZ и в WAN (Wide Area Network). 2.Из DMZ можно инициировать соединения в WAN. 3.Из WAN можно инициировать соединения в DMZ. 4.Инициация соединений из WAN и DMZ ко внутренней сети запрещена. 	Плюсы варианта предложенной схемы сети с DMZ: 1.Повышенная защищённость сети от взломов отдельных сервисов. Даже если один из серверов будет взломан, Нарушитель не сможет получить доступ к ресурсам, находящимся во внутренней сети (например, сетевым принтерам, системам видеонаблюдения и т.д.). Минусы варианта: 1.Сам по себе вынос серверов в DMZ не повышает их защищенность. Необходим дополнительный МЭ для отделения DMZ от внутренней сети.
25.	На рисунке представлена схема сети с DMZ. Общая схема работы данного варианта выглядит следующим образом:	Важные положительные свойства использования OpenVPN в данной схеме сети: 1. Кроссплатформенность.

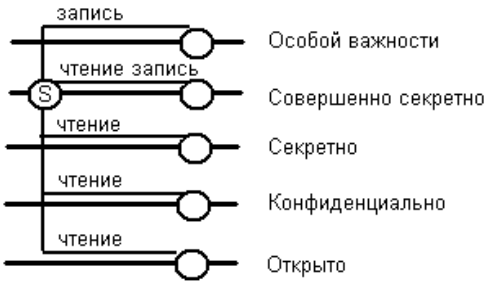
Номер задания	Содержание вопроса	Правильный ответ на задание
	1.На сервер в DMZ инсталлируется SSH/VPN сервер, а на сервер во внутренней сети инсталлируется SSH/VPN клиент. 2.Сервер внутренней сети инициирует построение сетевого туннеля до сервера в DMZ. Туннель строится с взаимной аутентификацией клиента и сервера. 3.Сервер из DMZ в рамках построенного туннеля инициирует соединение до сервера во внутренней сети, по которому передаются защищаемые данные. 4.На сервере внутренней сети настраивается локальный межсетевой экран, фильтрующий трафик, проходящий по туннелю. Перечислите положительные свойства использования OpenVPN, 	2. Возможность построения туннелей с взаимной аутентификацией клиента и сервера. 3. Возможность использования сертифицированной криптографии.
26.	Дайте описание понятию Гамма шифра.	Гамма шифра – псевдослучайная последовательность, вырабатываемая по определенному алгоритму, используемая для зашифровки открытых данных и дешифровки шифротекста. Используется при шифровании методом гаммирования.
27.	Опишите понятие криптоаналитическая атака компьютерной сети.	Любая попытка со стороны злоумышленника расшифровать шифротекст C и получить открытый текст M не имея подлинного ключа, называется криптоаналитической атакой.
28.	Перечислите основные принципы используемые при построении стойких шифров.	При построении стойких шифров необходимо использовать два основных принципа – рассеивание и перемешивание.
29.	Механизмы безопасной удаленной аутентификации пользователей.	Для обеспечения подлинности канала связи, и защиты от атак повторами обычно используют метод запрос-ответ, либо механизм отметки времени.
30.	Приведите не менее трех протоколов удаленной аутентификации пользователей.	Три примера можно выбрать из данного списка протоколов удаленной аутентификации пользователей: - CHAP - EAP - IPSec

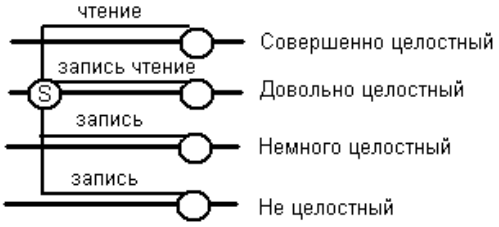
Номер задания	Содержание вопроса	Правильный ответ на задание
		- SSH - TLS v 1.2
31.	Приведите не менее трех изменений при динамической сегментации сети	Три примера можно выбрать из данного списка изменений при динамической сегментации сети: - правила контроля доступа; - состав групп пользователей; - местонахождение групп пользователей и т.д.
32.	Перечислите условия для проведения сегментации сети с использованием стандарта 802.1Q	Для проведения сегментации с использованием стандарта 802.1Q необходимо: - Четкая адресация сети, маски, network address, broadcast address. - Принцип логического разделения сети: по отделам, этажам, типу трафика и т.д. В одном сегменте рекомендуется держать не более 126 устройств. - Коммутаторы, поддерживающие 802.1Q. Маршрутизатор с поддержкой 802.1Q.
33.	Поставлена задача: Организовать определение принадлежность пользователя к нужной группе при его подключении к сети. Опишите кратко ваши предложения по решению данной задачи.	Данная задача обычно решается с помощью аутентификации и авторизации с использованием протокола 802.1x на RADIUS-сервере (часто с использованием данных из корпоративной службы каталогов, например Active Directory). Возможно применение и других методов — статического помещения пользователей в зависимости от порта подключения, VLAN’а, IP-подсети, авторизации по MAC-адресу и так далее в зависимости от возможностей используемого сервера AAA и оборудования.
34.	Поставлена задача: Изолировать трафик пользователя группы1 от трафика пользователей других групп при передаче по сети.	Данная задача традиционно решается путем создания отдельных виртуальных топологий для каждой группы пользователей. Как правило, это делается с помощью тех или иных средств виртуализации сети. В случае небольших сетей этими средствами обычно являются VLAN’ы и транки 802.1Q. Для больших сетей характерно применение MPLS VPN.
35.	Поставлена задача: Обеспечить доступ пользователя к тем ресурсам, к которым он должен иметь доступ и, заблокировать доступ ко всем остальным ресурсам	Данная задача как правило, решается пакетной фильтрацией на основе IP-адресов. Контроль доступа может быть реализован как такими «грубыми»

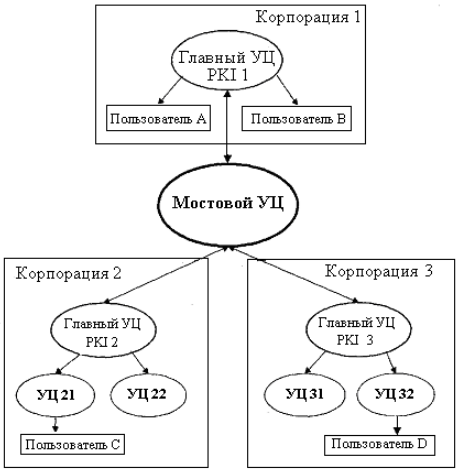
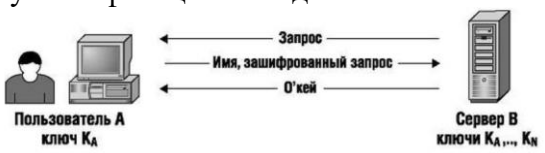
Номер задания	Содержание вопроса	Правильный ответ на задание
		средствами, как списки контроля доступа (ACL) на элементах сетевой инфраструктуры, так и «тонкой» фильтрацией на системах защиты нового поколения (NGFW, NGIPS),
36.	Перечислите виды ACL	Списки доступа бывают: Стандартные Расширенные Динамические Рефлексивные Повременные
37.	Перечислите два основных способа позволяющих устанавливать членство в VLAN.	Существуют два основных способа, позволяющих устанавливать членство в VLAN: 1) статические VLAN; 2) динамические VLAN.
38.	Возможно ли использование VLANов как метода защиты от широковещательного шторма?	Одним из методов защиты от широковещательного шторма является разделение сети на VLANы или на различные сети канального уровня, что локализует шторм в пределах одного VLAN/одной подсети.
39.	На рисунке представлена схема сети. Опишите какие необходимы настройки для исключения широковещательного шторма в петле. 	Необходимо настроить протокол STP стандарте IEEE 802.1D или протоколы семейства STP (RSTP, MST).
40.	Для чего в сетях используют Алгоритм связующего дерева (Spanning-Tree Algoritm) (sta)	Алгоритм STA предусматривает свободное от петель подмножество топологии сети путем размещения таких мостов, которые, если они включены, то образуют петли в резервном (блокирующем) состоянии. Порты блокирующего моста могут быть активированы в случае отказа основного канала, обеспечивая новый тракт через объединенную сеть.
41.	Перечислите возможные решения обеспечения безопасности корпоративной сети на основе D-Link.	D-Link предлагает комплексный подход к решению вопросов обеспечения безопасности, который включает в себя следующие решения: 1) Защита конечного пользователя — обеспечивает защиту внутренней сети от внутренних атак; 2) Защита средствами межсетевых

Номер задания	Содержание вопроса	Правильный ответ на задание
		экранов — обеспечивает защиту внутренней сети от внешних атак; 3) Объединенная безопасность — связующее звено между двумя предыдущими предложениями, объединяющее использование межсетевых экранов и коммутаторов для защиты сети.
42.	Какой функцией в коммутаторах D-Link реализован контролировать доступа компьютеров в сеть на основе их IP- и MAC-адресов.	Функция IP-MAC-Port Binding (IMPB), реализованная в коммутаторах D-Link, позволяет контролировать доступ компьютеров в сеть на основе их IP- и MAC-адресов, а также порта подключения.
43.	При активизации функции IMPB на порте администратор должен указать режим его работы. Как работает порт в режиме Strict Mode?	Strict Mode — в этом режиме порт по умолчанию заблокирован.
44.	При активизации функции IMPB на порте администратор должен указать режим его работы. Как работает порт в режиме Loose Mode?	Loose Mode — в этом режиме порт по умолчанию открыт.
45.	При активизации функции IMPB включен режим работы DHCP Snooping mode. Действия коммутатора в данном режиме?	Режим DHCP Snooping используется коммутатором для динамического создания записей IP-MAC на основе анализа DHCP-пакетов и привязки их к портам с включенной функцией IMPB (администратору не требуется создавать записи вручную).
46.	Одним из методов организации механизма ограничения административного доступа к управлению коммутатором является настройка коммутатора на работу с протоколом SSH. Опишите данный протокол.	SSH (Secure SHell, "безопасная оболочка") — сетевой протокол прикладного уровня, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений.
47.	Для чего используют физический стек коммутаторов 3-го уровня D-Link.	Под физическим стекированием понимается объединение нескольких коммутаторов в одно логическое устройство с целью увеличения количества портов, удобства управления и мониторинга. Объединенные в стек коммутаторы имеют общие таблицы коммутации и маршрутизации (для коммутаторов 3 уровня).
48.	В корпоративной сети при настройке коммутатора D-Link использовалась команда ip access-list std1 10. Для чего использовалась данная команда?	Команда ip access-list используется для создания именованных списков доступа, в данном случае создание списка с именем std1 и номером 10.
49.	В корпоративной сети при настройке	В данном случае создан расширенный

Номер задания	Содержание вопроса	Правильный ответ на задание
	коммутатора D-Link использовалась команда mac access-list extended mac1 6010. Для чего использовалась данная команда?	список доступа MAC с именем mac1 и номером 6010.
50.	Дайте описание понятия IPsec в рамках защиты информации в информационной системе.	IPsec (сокращение от IP Security) — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP.
51.	Выберите правильный вариант ответа. В вашей организации используются операционные системы Windows. Какая политика безопасности применима на данном предприятии? **A) ролевая политика безопасности** B) дискреционная политика безопасности C) Политика избирательного разграничения доступа D) мандатная модель управления доступом	A
52.	Выберите правильный вариант ответа. В информационно-коммуникационных средах операционной системой основанной на дискреционной политике безопасности, операционной системой является A) OS/2 **B) Linux** C) Windows D) SkyOS	B
53.	Выберите правильный вариант ответа. При организации безопасности доступа в информационно-коммуникационных средах протокол Диффи-Хеллмана используется при подходе к распределению ключевой информации в компьютерной сети. Этот подход называется A) Распределение ключевой информацией с использованием одного либо нескольких центров распределения ключей **B) Прямой обмен сеансовыми ключами между пользователями** C) Взаимное подтверждение подлинности участников сеанса D) подтверждение достоверности сеанса для защиты от атак методом повторов	B
54.	Выберите правильный вариант ответа. В модульной архитектуре системы защиты ПО от несанкционированного использования функции определения факта легальности запуска защищаемой программы, сравнивая текущие значения параметров среды с эталонными	C

Номер задания	Содержание вопроса	Правильный ответ на задание
	выполняет A) Блок установки характеристик среды B) Подсистема реализации защитных функций **C) Блок сравнения характеристик среды** D) Подсистема противодействия нейтрализации защитных механизмов	
55.	Выберите правильный вариант ответа. При организации безопасности доступа в информационных системах основными элементами поддержания изолированной программной среды являются A) поиском критических участков кода методом семантического анализа **B) контроль целостности и активности процессов** C) определение точки входа в ПЗУ D) защитой данных	B
56.	Выберите правильный вариант ответа. Нарушение конфиденциальности информационного обмена в ИС, осуществляемого по каналам связи абонентов систем и сетей организаций, с помощью их «прослушивания»; данный вид угроз для компьютерных сетей получил название A) Маскарад (spoofing) B) DoS атаками (DoS – Denied of Service) **C) Сниффинг (sniffing)** D) Фишинг (fishing)	C
57.	Выберите правильный вариант ответа. На рисунке показана схема демонстрации правила NWD (нет записи вниз). Какая политика безопасности поддерживает данное правило?  **A) политика безопасности Белла-ЛаПадулы** B) ролевая политика безопасности C) политика безопасности контроля целостности информационных ресурсов D) мандатная модель целостности Биба	A
58.	Выберите правильный вариант ответа.	D

Номер задания	Содержание вопроса	Правильный ответ на задание
	На рисунке показана схема демонстрации правила NWD (нет записи вверх). Какая политика безопасности поддерживает данное правило?  A) политика безопасности Белла-ЛаПадулы B) ролевая политика безопасности C) политика безопасности контроля целостности информационных ресурсов **D) мандатная модель целостности Биба**	
59.	Выберите правильный вариант ответа. Под _____ понимают подтверждение пользователем предъявленного идентификатора, проверка его подлинности и принадлежности именно данному пользователю. A) идентификация **B) аутентификацией** C) авторизация D) шифрование	B
60.	Выберите правильный вариант ответа. _____ — предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий A) идентификация B) аутентификацией **C) авторизация** D) шифрование	C
61.	Выберите правильный вариант ответа. Поставлена задача: Определить минимальную длину паролей L при мощности парольной системы A, обеспечивающих вероятность подбора пароля злоумышленником не более заданной P, при скорости подбора паролей V, максимальном сроке действия пароля T. Исходные данные – P=10-6, T=7 дней = 1 неделя, V=10 паролей / минуту = 10*60*24*7=100800 паролей в неделю, A=26 (символы английского алфавита). A) L=4	B

Номер задания	Содержание вопроса	Правильный ответ на задание
	B) L=8 C) L=6	
62.	Выберите правильный вариант ответа. Поставлена задача: Определить минимальную длину паролей L при мощности парольной системы A, обеспечивающих вероятность подбора пароля злоумышленником не более заданной P, при скорости подбора паролей V, максимальном сроке действия пароля T. Исходные данные – P=10-6, T=7 дней = 1 неделя, V=10 паролей / минуту = 10*60*24*7=100800 паролей в неделю, A=36 (малые латинские буквы и цифры). A) L=4 B) L=8 **C) L=6**	C
63.	Выберите правильный вариант ответа. На рисунке показана схема архитектуры  **A) Гибридная архитектура PKI (инфраструктура открытых ключей)** B) Централизованная архитектура PKI (инфраструктура открытых ключей) C) Блочная архитектура PKI (инфраструктура открытых ключей) D) Сертифицированная архитектура PKI (инфраструктура открытых ключей)	A
64.	Выберите правильный вариант ответа. На рисунке показана схема аутентификации методом  **A) «запрос-ответ»**	A

Номер задания	Содержание вопроса	Правильный ответ на задание
	B) неявного запроса C) Kerberos D) с использованием идентификационной таблицы	
65.	Выберите правильный вариант ответа. На рисунке показана схема аутентификации методом  **A) «запрос-ответ»** B) неявного запроса C) Kerberos D) с использованием идентификационной таблицы	-
66.	Дайте краткое описание понятию Формальные модели политик безопасности	Формальные модели политик безопасности позволяют описать поведение подсистемы безопасности в рамках строгих математических моделей, правил.
67.	Дайте краткое описание понятию Неформальные модели политик безопасности	Неформальные модели политик безопасности предполагают описание поведения подсистемы безопасности в рамках вербальных (словесных) утверждений, не обладающих математической строгостью.
68.	Перечислите основные множества ролевой политики безопасности в рамках которых осуществляется формализация.	Формализация ролевой модели осуществляется в рамках следующих множеств: 1) множество пользователей компьютерной системы. 2) множество ролей. 3) множество полномочий на доступ к объектам, представленное, например, в виде матрицы прав доступа. 4) множество сеансов работы пользователей с компьютерной системой.
69.	Опишите состав учетной записи пользователя	Совокупность идентификатора и пароля пользователя - основные составляющие его учетной записи.
70.	Что содержит База данных пользователей парольной системы?	База данных пользователей парольной системы содержит учетные записи всех пользователей корпоративной информационной системы.
71.	Приведите не менее трех широко	Три примера можно выбрать из

Номер задания	Содержание вопроса	Правильный ответ на задание
	распространенных технических устройств, используемых для решения задач идентификации/аутентификации пользователей	данного списка трех широко распространенных технических устройств, используемых для решения задач идентификации/аутентификации пользователей: - идентификаторы iButton (Touch Memory); - бесконтактные радиочастотные карты proximity; - пластиковые карты; - ключи e-Token.
72.	Перечислите процессы электронной цифровой подписи в соответствии с ГОСТ 34.10-2018.	Механизм цифровой подписи определяется посредством реализации двух основных процессов 1) формирование подписи; 2) проверка подписи.
73.	Назначение электронной цифровой подписи в соответствии с ГОСТ 34.10-2018.	Цифровая подпись предназначена для аутентификации лица, подписавшего электронное сообщение.
74.	Перечислите свойства сообщения при использовании электронной цифровой подписи в соответствии с ГОСТ 34.10-2018.	Использование ЭЦП предоставляет возможность обеспечить следующие свойства при передаче в системе подписанного сообщения: 1) осуществление контроля целостности передаваемого подписанного сообщения; 2) доказательное подтверждение авторства лица, подписавшего сообщение; 3) защита сообщения от возможной подделки.
75.	Дать описание понятию Дайджест Данных (Data Digest).	Дайджест Данных - Относительно небольшой блок данных, вычисленный с применением к оригинальному блоку данных (обычно большего размера) специальных дайджест-функций (хэш-функций).
76.	Задача: Предприятию необходимо получить квалифицированный электронный сертификат на организацию ЭЦП для защиты данных ИС. В какую организацию необходимо обратиться?	Аккредитованный удостоверяющий центр (УЦ) — это организация, получившая доступ к Единому реестру, имеющая право на сбор и хранение ключевой информации. Она имеет право на создание квалифицированного электронного сертификата и распространение лицензий на криптографию.
77.	Перечислите свойства информации с точки зрения Защиты информации	Свойства информации, которые могут приводить к потере ценности

Номер задания	Содержание вопроса	Правильный ответ на задание
		информации: 1) конфиденциальность; 2) целостность; 3) доступность.
78.	Перечислите стадии жизненного цикла вируса.	Жизненный цикл вирусов включает в себя две основные стадии – хранение (латентная фаза) и исполнение.
79.	Технические средства борьбы с компьютерными вирусами.	Технические средства борьбы с компьютерными вирусами – применение антивирусных мониторов и сканеров, программных и аппаратных средств, недопускающих возможность заражения объектов компьютерной системы.
80.	Перечислите виды источников угроз безопасности персональных данных.	Источники угроз безопасности персональных данных: 1. Антропогенные 2. Стихийные 3. Техногенные
81.	Дайте описание атакам MITM (Man-in-the-Middle).	Атака MITM происходит, когда хакеры внедряются в двустороннее информационное взаимодействие. После перехвата трафика они могут фильтровать и красть данные.
82.	Дайте описание атакам Фишинг	Вымогатели используют поддельные сообщения, например, e-mail, чтобы обманным путем заставить получателя открыть его и выполнить определенное действие.
83.	Приведите не менее трех биометрических характеристик, используемых для идентификации и аутентификации ИС.	Три примера можно выбрать из данного списка биометрических характеристик, используемых для идентификации и аутентификации ИС: - отпечатки пальцев; - геометрическая форма рук; - узор радужной оболочки и сетчатки глаз; - форма и размеры лица; - особенности голоса; - биомеханические характеристики почерка; - биомеханические характеристики «клавиатурного почерка».
84.	Перечислите особенности использования биометрических систем идентификации и аутентификации личности по сравнению с другими классами систем И/АУ.	Особенностью применения биометрических систем следующие: 1.Необходимость длительного обучения биометрической системы. 2.Возможность ошибочных отказов и

Номер задания	Содержание вопроса	Правильный ответ на задание
		ошибочных подтверждений при аутентификации пользователей. 3.Необходимость использования специальных технических устройств.
85.	Поставлена задача: Приобретение российской программы управления ключами для организации. Приведите примеры российских программ управления ключами.	Российские программы управления ключами: ViPNet PKI Client Guardant Sign семейство Крипто и т.д.
86.	Является ли обязательным предоставление физическими лицами своих биометрических персональных данных в соответствии с Федеральным законом от 29 декабря 2022 г. N 572-ФЗ	Предоставление физическими лицами своих биометрических персональных данных в целях, предусмотренных настоящим Федеральным законом, не может быть обязательным.
87.	Дайте описание понятию биометрический процесс в соответствии ГОСТ Р 54411-2018/ISO/IEC TR 24722:2015.	Биометрический процесс - автоматический процесс, использующий одну или более биометрических характеристик одного индивида для биометрической регистрации, верификации или идентификации.
88.	Дайте описание понятию Непрерывный биометрический параметр процесс в соответствии ГОСТ Р 52633.4-2011.	Непрерывным считается биометрический параметр, значения которого составляют континуальное множество и ограничены только точностью представления.
89.	Перечислите меры защиты программных продуктов используемые для противодействия попыткам несанкционированного использования программного обеспечения.	Для противодействия попыткам несанкционированного использования программного обеспечения используются следующие меры защиты программных продуктов: 1.Организационно-экономические меры 2.Правовые меры 3.Технические меры
90.	Перечислите типы систем защиты программного обеспечения по способу ассоциации (внедрения) защитного механизма.	Системы защиты ПО от несанкционированного использования по способу ассоциации (внедрения) защитного механизма можно подразделить на два типа: 1) встроенные системы (внедряются при создании ПО); 2) пристыковочные системы (подключаются к уже готовому ПО).
91.	Опишите основную функцию службы Active Directory (службы активного	Службы Active Directory (службы активного каталога) представляют

Номер задания	Содержание вопроса	Правильный ответ на задание
	каталога).	собой распределённую базу данных, которая содержит все объекты домена. Доменная среда Active Directory является единой точкой аутентификации и авторизации пользователей и приложений в масштабах предприятия.
92.	Дайте описание понятию контроллер домена в рамках Active Directory (службы активного каталога).	База данных Active Directory хранится на выделенных серверах – контроллерах домена
93.	Дайте описание понятию Группы безопасности в рамках Active Directory (службы активного каталога).	Группы безопасности — это способ сбора учетных записей пользователей, учетных записей компьютеров и других групп в управляемые единицы.
94.	Перечислите области действия групп Active Directory	Active Directory определяет следующие три области группы: 1.Универсальное. 2.Глобальный. 3.Локальный домен.
95.	Перечислите компоненты Active Directory	Active Directory включает в себя следующие компоненты: Объекты. Домены. Организационные единицы. Деревья. Леса.
96.	Задача: На нефтехимическом предприятии в медпункте предприятия с помощью медицинских информационных систем сотрудники медпункта обрабатывают персональные медицинские данные в МИС. Определите какой уровень защищенности необходимо организовать для выполнения ФЗ N 1119 от 01.11.2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».	В зависимости от количества обрабатываемых субъектов персональных данных и типа актуальных угроз безопасности в МИС требуется обеспечить второй или третий уровень защищенности персональных данных.
97.	Задача: На нефтехимическом дочернем предприятии ведется обработка бухгалтерских данных и затем по защищенному каналу передается в головное отделения предприятия. Работников дочернего предприятия более 100 000 субъектов. Определите какой уровень защищенности необходимо организовать для выполнения ФЗ N 1119 от 01.11.2012 «Об утверждении требований к защите персональных данных при их	В данном случае требуется обеспечить третий уровень защищенности персональных данных и выше.

Номер задания	Содержание вопроса	Правильный ответ на задание
	обработке в информационных системах персональных данных».	
98.	На складе предприятия по беспроводной сети передают информацию о принятых и отправленных грузах. Опишите методы защиты передаваемых данных по беспроводной сети.	В описываемой ситуации достаточно стандартных вариантов шифрования данных при передаче по беспроводной сети (протоколы WPA 3, CKIP, TKIP, AES-CCMP и т.д.).
99.	Поставлена задача: необходимо пошагово проанализировать работу ОС. На какие программные средства вы будите использовать?	Отладчики – программные средства, позволяющие выполнять программу в пошаговом режиме, контролировать ее выполнение, вносить изменения в ход выполнения.
100.	Поставлена задача: необходимо проанализировать работу реестра ОС Windows. На какие программные средства вы будите использовать?	Мониторы операций с реестром – предоставляет возможность собрать информацию об обращениях к реестру Windows.