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 26.05.2022г. № 05

Рабочая программа

Защита информации

Направление подготовки 09.03.01 Информатика и вычислительная техника

Квалификация (степень) выпускника – бакалавр

Форма обучения – очная, заочная, очно-заочная

Тольятти, 2022 г.

Рабочая программа **Защита информации** составлена с требованиями ФГОС, ВО, ОПОП по направлению подготовки 09.03.01 Информатика и вычислительная техника (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 № 10 от 20.05.2022г.

Зав. кафедрой ИиСУ, к.п.н., доцент Е.Н. Горбачевская

Одобрена Учебно-методическим советом вуза

протокол № 05 от 25.05.2022г

председатель Учебно-методического совета Н.Г. Рогова

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
Администрирование сетевой подсистемы инфокоммуникационной системы организации	ПК-2

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Данная учебная дисциплина относится к к части, формируемой участниками образовательных отношений 09.03.01 «Информатика и вычислительная техника».

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-2	Администрирование сетевой подсистемы инфокоммуникационной системы организации	Операционные системы Linux и системы реального времени Системное программное обеспечение Сети и телекоммуникации	Микропроцессорные системы Проектирование вычислительных систем и комплексов Корпоративные сети/Промышленные сети Производственная практика. Технологическая (проектно-технологическая) практика Преддипломная 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-2. Администрирование сетевой подсистемы инфокоммуникационной системы организации	ПК-2.1. Анализирует принципы функционирования аппаратных, программных и программно-аппаратных средств сетевой подсистемы инфокоммуникационной системы организации ПК-2.2. Проектирует архитектуру аппаратных, программных и программно-аппаратных средств сетевой подсистемы инфокоммуникационной системы организации ПК-2.3. Применяет сетевые модели OSI и IEEE, структуру и основные принципы работы сети Интернет ПК-2.6. Использует современные стандарты, нормативно-техническую документацию в области инфокоммуникационных технологий при администрировании устройств и программного обеспечения ПК-2.7. Участвует в проектировании, конфигурировании и планировании с требуемой производительностью и необходимой безопасностью сетевых подсистем инфокоммуникационной системы организации ПК-2.8. Участвует в настройке, администрировании, восстановлении при сбоях аппаратных, программных и программно-аппаратных средств сетевой подсистемы инфокоммуникационной системы организации

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	2			3

	распределение ключевой информации. Протоколы 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	1			8

	программного обеспечения от несанкционированного использования				
8	Тема 8. Защита от разрушающих программных воздействий	1			8
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	2		16	7

	в компьютерных сетях				
10	Тема 10. Инженерно-техническая защита информации	2			7
11	Тема 11. Руководящие документы России. Правовое обеспечение информационной безопасности и противодействию терроризму.	2			6
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

*В ДАННЫЙ ПУНКТ ВНЕСЕНЫ ИЗМЕНЕНИЯ ОБНОВЛЕННОЙ ЛИТЕРАТУРЫ

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

09.03.01 «Информатика и вычислительная техника»

Квалификация (степень) выпускника – бакалавриат

Тольятти 2022

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-2. Администрирование сетевой подсистемы инфокоммуникационной системы организации	ПК-2.1. Анализирует принципы функционирования аппаратных, программных и программно-аппаратных средств сетевой подсистемы инфокоммуникационной системы организации ПК-2.2. Проектирует архитектуру аппаратных, программных и программно-аппаратных средств сетевой подсистемы инфокоммуникационной системы организации ПК-2.3. Применяет сетевые модели OSI и IEEE, структуру и основные принципы работы сети Интернет ПК-2.6. Использует современные стандарты, нормативно-техническую документацию в области инфокоммуникационных технологий при администрировании устройств и программного обеспечения ПК-2.7. Участвует в проектировании, конфигурировании и планировании с требуемой производительностью и необходимой безопасностью сетевых подсистем инфокоммуникационной системы организации ПК-2.8. Участвует в настройке, администрировании, восстановлении при сбоях аппаратных, программных и программно-аппаратных средств сетевой подсистемы инфокоммуникационной системы организации

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

Результаты обучения по дисциплине «Защита информации» направления подготовки 09.03.01 «Информатика и вычислительная техника» 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	Оценочное	Экзамен (вопросы к экзамену)

	средство 1 (лабораторное задания)	средство 2	
ПК-2	ПК-2.1. ПК -2.2. ПК -2.3. ПК -2.6. ПК -2.7. ПК -2.8.		ПК-2.1. ПК -2.2. ПК -2.3. ПК -2.6. ПК -2.7. ПК -2.8.

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

3.1 Перечень вопросов для промежуточной аттестации (экзамен)

Основные понятия и определения предмета защиты информации. Санкционированный и несанкционированный доступ. Базовые свойства безопасности информации. Угрозы безопасности и каналы реализации угроз.

Основные понятия и определения предмета защиты информации. Основные принципы обеспечения информационной безопасности. Ценность информации.

Основные понятия и определения предмета защиты информации. Меры обеспечения безопасности компьютерных систем. Характеристика способов защиты компьютерной информации с помощью аппаратно-программных мер.

Разграничение доступа к ресурсам. Политики безопасности. Классификация политик безопасности.

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

Идентификация и аутентификация субъектов. Классификация подсистем идентификации и аутентификации субъектов. Парольные системы идентификации и аутентификации пользователей.

Идентификация и аутентификация субъектов. Идентификация и аутентификация пользователей с использованием технических устройств. Идентификация и аутентификация с использованием индивидуальных биометрических характеристик пользователя.

Методы и средства криптографической защиты. Принципы криптографической защиты информации.

Методы и средства криптографической защиты. Традиционные симметричные криптосистемы: шифрование методом замены, шифрование методами перестановки, шифрование методом гаммирования. Элементы криптоанализа.

Методы и средства криптографической защиты. Современные симметричные системы шифрования: стандарт шифрования DES (США), отечественный стандарт симметричного шифрования.

Методы и средства криптографической защиты. Асимметричные криптосистемы: недостатки симметричных криптосистем и принципы асимметричного шифрования, однонаправленные функции, алгоритм шифрования RSA.

Контроль целостности информации. Электронно-цифровая подпись. Проблема обеспечения целостности информации.

Контроль целостности информации. Электронно-цифровая подпись. Функции хэширования и электронно-цифровая подпись.

Контроль целостности информации. Электронно-цифровая подпись. Инфраструктура открытых ключей PKI.

Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей. Типовые схемы хранения ключевой информации.

Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей. Защита баз данных аутентификации в ОС Windows и UNIX.

Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей. Иерархия ключевой информации. Распределение ключей.

Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей. Протоколы безопасной удаленной аутентификации пользователей.

Защита программного обеспечения от несанкционированного использования. Проблема защиты программного обеспечения от несанкционированного использования.

Защита программного обеспечения от несанкционированного использования. Модульная архитектура технических средств защиты ПО от несанкционированного использования.

Защита программного обеспечения от несанкционированного использования. Функционирование подсистем и модулей системы защиты ПО от несанкционированного использования.
Защита программного обеспечения 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.
Защита от разрушающих программных воздействий. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и РПВ.
Защита от разрушающих программных воздействий. Компьютерные вирусы как класс РПВ. Защита от РПВ. Изолированная программная среда.
Защита информации в компьютерных сетях. Основные угрозы и причины уязвимости сети INTERNET.
Защита информации в компьютерных сетях. Классификация типовых удаленных атак на интрасети. Подходы к защите от типовых удаленных атак.
Защита информации в компьютерных сетях. Ограничение доступа в сеть. Межсетевые экраны. Виртуальные частные сети (VPN).
Защита информации в компьютерных сетях. Доменная архитектура в Windows NT. Служба Active Directory.
Защита информации в компьютерных сетях. Централизованный контроль удаленного доступа. Серверы аутентификации.
Инженерно-техническая защита информации. Радиомикрофоны. Устройства перехвата телефонных сообщений.
Инженерно-техническая защита информации. Специализированные устройства. Обнаружение, локализация и подавление закладных подслушивающих устройств.
Инженерно-техническая защита информации. Предотвращение утечки информации через побочные электромагнитные излучения и наводки.
Руководящие документы России. Правовое обеспечение информационной безопасности и противодействию терроризму. Показатели защищенности средств вычислительной техники от НСД.
Правовое обеспечение информационной безопасности и противодействию терроризму. 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.
Правовое обеспечение информационной безопасности и противодействию терроризму. Законодательное противодействие распространению террористических материалов в Интернет.
Правовое обеспечение информационной безопасности и противодействию терроризму. Проблемы экспертизы информационных материалов, содержащих признаки идеологии терроризма.

3.3 Оценочное средство 1 (лабораторное задания)

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

Критерии конкретного оценочного средства (согласно ПОЛОЖЕНИЮ о промежуточной аттестации обучающихся ВУиТ по программам высшего образования – программам бакалавриата и программам специалитета)

По итогам тестирования оценка знаний обучающегося производится в соответствии со следующими критериями:

правильных ответов 0-39% – «неудовлетворительно»/«не зачтено»;
правильных ответов 40-59% – «удовлетворительно»/«зачтено»;
правильных ответов 60-79% – «хорошо»/«зачтено»;
правильных ответов 80-100% – «отлично»/«зачтено».

Тесты

Тесты АСТ установлены в Центре тестирования по адресу Белорусская 16, ауд 104