МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ – МСХА имени К.А. ТИМИРЯЗЕВА»
(ФГБОУ ВО РГАУ - МСХА имени К.А. Тимирязева)

Институт Экономики и управления АПК
Кафедра прикладной информатики

УТВЕРЖДАЮ:
Директор института
экономики и управления АПК
_____ Л.И. Хоружий
"__28__" ____08_____ 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.03.01 Безопасность и защита информационных систем

для подготовки бакалавров

ФГОС ВО

Направление: 44.03.04 Профессиональное обучение (по отраслям)
Направленность: «Информационные системы и технологии»

Курс 4
Семестр 7

Форма обучения: очная

Год начала подготовки: 2025

Москва, 2025

Разработчик (и): Пчелинцева С.В., к.т.н., доцент
(ФИО, ученая степень, ученое звание) (подпись)

(ФИО, ученая степень, ученое звание) (подпись)

« 28 » августа 2025 г.

Рецензент: Ашмарина Т.И., к.э.н, доцент
(ФИО, ученая степень, ученое звание) (подпись)

« 28 » августа 2025 г.

Программа составлена в соответствии с требованиями ФГОС ВО, профессионального стандарта и учебного плана по направлению подготовки 44.03.04 Профессиональное обучение (по отраслям).

Программа обсуждена на заседании кафедры прикладной информатики протокол №1 от « 28 » августа 2025 г.

И.о. зав. кафедрой прикладной информатики Худякова Е.В., д.э.н., профессор
(ФИО, ученая степень, ученое звание) (подпись)

«« 28 » августа 2025 г.

Согласовано:

Председатель учебно-методической комиссии института экономики и управления АПК
Гупалова Т.Н., к.э.н., доцент
(ФИО, ученая степень, ученое звание) (подпись)

« 28 » августа 2025 г.

И.о. заведующего выпускающей кафедрой Прикладной информатики Худякова Е.В., д.э.н., проф.
(ФИО, ученая степень, ученое звание) (подпись)

« 28 » августа 2025 г.

Заведующий отделом комплектования ЦНБ

СОДЕРЖАНИЕ

Аннотация
рабочей программы учебной дисциплины (индекс) Б1.В.03.01 Безопасность и защита информационных систем для подготовки бакалавра по направлению 44.03.04 Профессиональное обучение (по отраслям) направленности «Информационные системы и технологии»

Цель освоения дисциплины: формирование у студентов компетенций в области информационной безопасности, а также развитие способности оценивать риски и разрабатывать меры защиты информации в различных информационных системах. Студенты должны овладеть методами защиты данных, средствами защиты сетевых и программных ресурсов, а также основами обеспечения конфиденциальности, целостности и доступности информации.

Место дисциплины в учебном плане: дисциплина включена в часть, формируемую участниками образовательных отношений учебного плана по направлению подготовки 44.03.04 Профессиональное обучение (по отраслям).

Требования к результатам освоения дисциплины: в результате освоения дисциплины формируются следующие компетенции (индикаторы): ПКос-2.1; ПКос-2.2; ПКос-2.3.

Краткое содержание дисциплины:

Принципы построения компьютерных сетей. Типовая IP-сеть организации. Классификация сетевых уязвимостей и атак. Работа с базами атак и уязвимостей. Защитные механизмы и средства обеспечения безопасности. Базовые принципы сетевого взаимодействия. Стек сетевых протоколов операционных систем. Принципы функционирования сетевых протоколов, включающих криптографические алгоритмы. Риски, угрозы, уязвимости, атаки. Встроенные средства защиты в ОС. Идентификация и аутентификация. Разграничение доступа к ресурсам. Защита сетевого взаимодействия. Повышение уровня защищенности рабочей среды пользователей.

Общая трудоемкость дисциплины: 108/3 (часы/зач. ед.).

Промежуточный контроль: экзамен в 7 семестре.

1. Цель освоения дисциплины

Целью освоения дисциплины «Безопасность и защита информационных систем» является формирование у студентов знаний и навыков в области информационной безопасности, необходимых для обеспечения защиты информации в современных информационных системах. Студенты изучат основные угрозы информационной безопасности, методы и средства защиты данных, а также принципы обеспечения конфиденциальности, целостности и доступности информации. Особое внимание будет уделено защите информации в сетевых и распределенных системах, а также управлению рисками безопасности. В рамках дисциплины студенты научатся анализировать возможные угрозы и разрабатывать эффективные меры защиты для предотвращения утечек и атак. Освоение дисциплины также включает изучение актуальных стандартов и нормативных актов в области информационной безопасности.

2. Место дисциплины в учебном процессе

Дисциплина «Безопасность и защита информационных систем» включена в часть, формируемую участниками образовательных отношений учебного плана направления 44.03.04 Профессиональное обучение (по отраслям), осваивается в 7 семестре. Дисциплина «Безопасность и защита информационных систем» реализуется в соответствии с требованиями ФГОС ВО, ОПОП ВО и Учебного плана по направлению 44.03.04 Профессиональное обучение (по отраслям). Предшествующими дисциплинами, на которых базируется дисциплина Электронные образовательные ресурсы, Математика, Информатика.

Рабочая программа дисциплины «Безопасность и защита информационных систем» для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Образовательные результаты освоения дисциплины обучающимся, представлены в таблице 1.

Таблица 1

Требования к результатам освоения учебной дисциплины

№ п/п	Код компетенции	Содержание компетенции (или её части)	Индикаторы компетенций	В результате изучения учебной дисциплины обучающиеся должны:		
				знать	уметь	владеть
1	ПКос-2	2Способен выполнять деятельность и (или) демонстрировать элементы осваиваемой обучающимися деятельности, предусмотренной программой учебной дисциплины (модуля), прак-	ПКос-2.1 Знает: современные информационные технологии и программные средства, методы алгоритмизации, языки и системы программирования, основные платформы, технологии и инструментальные программно-аппаратные средства для реализации информационных систем в сфере образования	современные информационные технологии и программные средства, методы алгоритмизации, языки и системы программирования, основные платформы, технологии и инструментальные программно-аппаратные средства для реализации информационных систем в сфере образования	-	-

		тики	ПКос-2.2; Умеет: выбирать современные информационные технологии и программные средства, применять методы алгоритмизации, языки и системы программирования, осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем при решении профессиональных задач в сфере образования	-	выбирать современные информационные технологии и программные средства, применять методы алгоритмизации, языки и системы программирования, осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем при решении профессиональных задач в сфере образования	-
			ПКос-2.3 Владеет: навыками применения современных информационных технологий и программных средств, навыками программирования и инструментальными программно-аппаратными средствами в сфере образования	-	-	навыками применения современных информационных технологий и программных средств, навыками программирования и инструментальными программно-аппаратными средствами в сфере образования

4. Структура и содержание дисциплины

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 3 зач. единицы (108 часов), их распределение по видам работ в 7 семестре представлено в табл. 2.

Таблица 2

Распределение трудоёмкости дисциплины по видам работ по семестрам

Вид учебной работы	Трудоёмкость	
	час.	в т.ч. в семестре № 7
Общая трудоёмкость дисциплины по учебному плану	**108**	**108**
1. Контактная работа:	**52,4**	**52,4/4**
Аудиторная работа	**52,4**	**52,4/4**
лекции (Л)	16	16
практические занятия (ПЗ)	34	34/4
контактная работа на промежуточном контроле (КРА)	0,4	0,4
консультация	2	2
2. Самостоятельная работа (СРС)	**19,6**	**19,6**
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к практическим занятиям и т.д.)		
Подготовка к экзамену (контроль)	36	36
Вид промежуточного контроля	экзамен	

4.2 Содержание дисциплины

Тематический план учебной дисциплины

Таблица 3

Наименование разделов и тем дисциплины	Всего часов на раздел	Аудиторная работа			Внеаудиторная работа
		Л	ПЗ	ПКР	СР
Тема 1. Принципы построения компьютерных сетей и базовые принципы сетевого взаимодействия	8	2	4	-	2
Тема 2. Сетевые уязвимости, атаки и методы их обнаружения	10	2	4	-	4
Тема 3. Безопасность физических и канальных уровней сети	16	4	8	-	4
Тема 4. Защита периметра и трафика сети	16	4	8	-	4

Наименование разделов и тем дисциплины	Всего часов на раздел	Аудиторная работа			Внеаудиторная работа
		Л	ПЗ	ПКР	СР
Тема 5. Анализ защищённости сети и превентивные механизмы защиты	10	2	6	-	2
Тема 6. Угрозы безопасности и встроенные средства защиты операционных систем	9,6	2	4	-	3,6
Контактная работа на промежуточном	0,4	-	-	0,4	-
Экзамен, консультация перед экзаменом	38	-	-	38	-
Итого по дисциплине	**108**	**16**	**34**	**38,4**	**19,6**

Тема 1. Принципы построения компьютерных сетей и базовые принципы сетевого взаимодействия

Основные принципы построения компьютерных сетей, модели OSI и TCP/IP, компоненты типовой IP-сети организации, маршрутизация и управление трафиком, протоколы передачи данных, назначение и структура подсетей, базовые принципы сетевого взаимодействия, технологии коммутации и маршрутизации.

Тема 2. Сетевые уязвимости, атаки и методы их обнаружения

Классификация сетевых уязвимостей, типы атак (пассивные, активные, внутренние, внешние), работа с базами данных атак и уязвимостей (CVE), типичные уязвимости приложений (DNS, HTTP, FTP), системы обнаружения вторжений (IDS), методы анализа сетевого трафика, признаки сетевых атак, предотвращение распространённых атак (DDoS, атаки на пароли, SQL-инъекции).

Тема 3. Безопасность физических и канальных уровней сети

Проблемы физической безопасности сети, защита оборудования от несанкционированного доступа, уязвимости протокола ARP, защита на канальном уровне, применение стандарта 802.1x, механизмы контроля доступа на уровне порта, проблемы безопасности беспроводных сетей, физическое разделение сетей, защита каналов связи.

Тема 4. Защита периметра и трафика сети

Основы защиты периметра сети, межсетевые экраны и их конфигурация, системы предотвращения вторжений (IPS), защита трафика на сетевом уровне (VPN, IPsec), шифрование данных, безопасность транспортного уровня (TLS/SSL), фильтрация трафика, анализ маршрутов и управление политиками доступа, предотвращение утечек данных.

Тема 5. Анализ защищённости сети и превентивные механизмы защиты

Методы тестирования сети на наличие уязвимостей, инструменты анализа защищённости (Nmap, Wireshark), аудит безопасности сети, разработка превентивных мер, составление отчётов по защищённости, оценка рисков, мониторинг активности пользователей, анализ сетевых логов, применение рекомендаций по повышению уровня защищённости сети.

Тема 6. Угрозы безопасности и встроенные средства защиты операционных систем

Изучаются риски, угрозы и уязвимости операционных систем, а также способы их минимизации. Анализируются встроенные средства защиты операционных систем, включая антивирусы, межсетевые экраны, механизмы разграничения доступа и встроенные функции мониторинга безопасности.

4.3 Лекции/практические занятия

Таблица 4

Содержание лекций/практических занятий и контрольные мероприятия

№ п/п	Название раздела, темы	№ и название лекций/ лабораторных/ практических/ семинарских занятий	Формируемые компетенции	Вид контрольного мероприятия	Кол-во Часов/ из них практическая подготовка
1.	**Раздел 1.** Основы и теоретические аспекты цифровой трансформации				
	Тема 1. Принципы построения компьютерных сетей и базовые принципы сетевого взаимодействия	Лекция № 1. Принципы построения компьютерных сетей и основы сетевого взаимодействия	ПКос-2.1; ПКос-2.2; ПКос-2.3.	Устный опрос	2
	Тема 2. Сетевые уязвимости, атаки и методы их обнаружения	Лекция № 2. Сетевые уязвимости, атаки и методы их обнаружения	ПКос-2.1; ПКос-2.2; ПКос-2.3.	Устный опрос	2
		Практическое занятие № 2. Сетевые уязвимости, атаки и методы их обнаружения	ПКос-2.1; ПКос-2.2; ПКос-2.3.		
	Тема 3. Безопасность физических и канальных уровней сети	Лекция № 3. Безопасность физических и канальных уровней сети	ПКос-2.1; ПКос-2.2; ПКос-2.3.	Устный опрос	2
		Практическое занятие № 3. Оценка уязвимостей и методов защиты физических и канальных уровней сети	ПКос-2.1; ПКос-2.2; ПКос-2.3.	Защита практической работы № 1	2
	Тема 4. Защита периметра и трафика сети	Лекция № 4. Защита периметра и трафика сети	ПКос-2.1; ПКос-2.2; ПКос-2.3.	Защита	2
		Практическое занятие № 4. Защита периметра и трафика сети	ПКос-2.1; ПКос-2.2; ПКос-2.3.	практической работы № 2	
	Тема 5. Анализ защи-	Лекция № 5.Анализ защищённости сети и превентив-	ПКос-2.1; ПКос-2.2;	Защита практиче	2

	щённости сети и превентивные механизмы защиты	ные механизмы защиты	ПКос-2.3.		
		Практическое занятие № 5. Оценка защищённости сети и	ПКос-2.1; ПКос-2.2; ПКос-2.3.	ской работы № 3	
2.	**Раздел 2.** Оценка экономической эффективности ИТ и ИС				
	Тема 6. Угрозы безопасности и встроенные средства защиты операционных систем	Лекция 6. Угрозы безопасности и встроенные средства защиты операционных систем	ОПК-4.3, УК-10.1	Защита практиче	2
		Практическое занятие № 4. Анализ угроз безопасности и настройка встроенных средств защиты операционных систем		ской работы № 4	

Таблица 5

Перечень вопросов для самостоятельного изучения дисциплины

№ п/п	Название раздела, темы	Перечень рассматриваемых вопросов для самостоятельного изучения
1.	Тема 1. Принципы построения компьютерных сетей и базовые принципы сетевого взаимодействия	Основные принципы построения компьютерных сетей, модели OSI и TCP/IP, компоненты типовой IP-сети организации, маршрутизация и управление трафиком, протоколы передачи данных, назначение и структура подсетей, базовые принципы сетевого взаимодействия, технологии коммутации и маршрутизации (ПКос-2.1; ПКос-2.2; ПКос-2.3.).
2.	Тема 2. Сетевые уязвимости, атаки и методы их обнаружения	Классификация сетевых уязвимостей, типы атак (пассивные, активные, внутренние, внешние), работа с базами данных атак и уязвимостей (CVE), типичные уязвимости приложений (DNS, HTTP, FTP), системы обнаружения вторжений (IDS), методы анализа сетевого трафика, признаки сетевых атак, предотвращение распространённых атак (DDoS, атаки на пароли, SQL-инъекции) (ПКос-2.1; ПКос-2.2; ПКос-2.3.).
3.	Тема 3. Безопасность физических и канальных уровней сети	Проблемы физической безопасности сети, защита оборудования от несанкционированного доступа, уязвимости протокола ARP, защита на канальном уровне, применение стандарта 802.1x, механизмы контроля доступа на уровне порта, проблемы безопасности беспроводных сетей, физическое разделение сетей, защита каналов связи (ПКос-2.1; ПКос-2.2; ПКос-2.3.).
4.	Тема 4. Защита периметра и трафика сети	Основы защиты периметра сети, межсетевые экраны и их конфигурация, системы предотвращения вторжений (IPS), защита трафика на сетевом уровне (VPN, IPsec), шифрование данных, безопасность транспортного уровня (TLS/SSL), фильтрация трафика, анализ маршрутов и управление политиками доступа, предотвращение утечек данных (ПКос-2.1;

№ п/п	Название раздела, темы	Перечень рассматриваемых вопросов для самостоятельного изучения
		ПКос-2.2; ПКос-2.3.).
5.	Тема 5. Анализ защищённости сети и превентивные механизмы защиты	Методы тестирования сети на наличие уязвимостей, инструменты анализа защищённости (Nmap, Wireshark), аудит безопасности сети, разработка превентивных мер, составление отчётов по защищённости, оценка рисков, мониторинг активности пользователей, анализ сетевых логов, применение рекомендаций по повышению уровня защищённости сети (ПКос-2.1; ПКос-2.2; ПКос-2.3.).
6.	Тема 6. Угрозы безопасности и встроенные средства защиты операционных систем	Что включает в себя техническое задание на разработку информационной системы. Этапы разработки ТЗ. Методология и стандарты разработки ТЗ. Влияние требований заказчика на содержание ТЗ. Риски, связанные с недостаточной проработкой ТЗ (ПКос-2.1; ПКос-2.2; ПКос-2.3.).

5. Образовательные технологии

Таблица 6

Применение активных и интерактивных образовательных технологий

№ п/п	Тема и форма занятия		Наименование используемых активных и интерактивных образовательных технологий
1.	Принципы построения компьютерных сетей и базовые принципы сетевого взаимодействия	Л	Лекция-визуализация
2.	Сетевые уязвимости, атаки и методы их обнаружения	Л	Лекция-визуализация
3.	Безопасность физических и канальных уровней сети	Л	Лекция-визуализация
		ПЗ	Проблемно-поисковое занятие, творческие задания, групповое обсуждение
4.	Защита периметра и трафика сети	ПЗ	Проблемно-поисковое занятие, творческие задания, групповое обсуждение
5.	Анализ защищённости сети и превентивные механизмы защиты	ПЗ	Проблемно-поисковое занятие, творческие задания, групповое обсуждение
6.	Угрозы безопасности и встроенные средства защиты операционных систем	ПЗ	Проблемно-поисковое занятие, творческие задания, групповое обсуждение

6. Текущий контроль успеваемости и промежутзаочная аттестация по итогам освоения дисциплины

6.1 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности

6.1.1 Вопросы для устного опроса

Устный опрос проводится по первой, второй и третьей темам дисциплины «Безопасность и защита информационных систем».

Тема 1. Принципы построения компьютерных сетей и базовые принципы сетевого взаимодействия

1. Что такое компьютерная сеть и какие основные типы сетей существуют?
2. Какие принципы лежат в основе построения локальных и глобальных компьютерных сетей?
3. Каковы основные компоненты компьютерной сети и их функции?
4. Что такое модель OSI и как она используется для организации сетевого взаимодействия?
5. Какие функции выполняют канальный и сетевой уровни модели OSI?
6. В чем заключается принцип адресации в компьютерных сетях?
7. Как происходит обмен данными между узлами сети и что такое протоколы связи?
8. Чем отличается коммутация пакетов от коммутации цепей в компьютерных сетях?
9. Какую роль в сетевом взаимодействии играет IP-адресация?
10. Что такое шлюз и как он используется для подключения различных сетей?

Тема 2. Сетевые уязвимости, атаки и методы их обнаружения

1. Что такое сетевые уязвимости и как они могут быть использованы злоумышленниками?
2. Какие виды атак на компьютерные сети существуют и как они классифицируются?
3. Что такое атака "отказ в обслуживании" (DoS) и как она влияет на функционирование сети?
4. Каковы особенности атак "человек посередине" (MITM) и методы их предотвращения?
5. Что такое SQL-инъекция и как она может быть использована для атак на сети?
6. Какие методы используются для обнаружения сетевых уязвимостей и их устранения?
7. Что такое сетевой сканер и как он используется для поиска уязвимостей в сети?
8. Какую роль в защите сети играют системы обнаружения вторжений (IDS)?
9. Какова разница между активными и пассивными методами обнаружения сетевых атак?
10. Что такое уязвимость нулевого дня (zero-day) и как она может повлиять на безопасность сети?

Тема 3. Безопасность физических и канальных уровней сети

1. Что такое физический уровень сети и какие угрозы безопасности могут возникать на этом уровне?
2. Каковы основные методы защиты канала связи на канальном уровне?
3. В чем заключается роль криптографических технологий в обеспечении безопасности на физическом уровне сети?

4. Какую роль в безопасности канала связи играет метод доступа к среде передачи данных (например, CSMA/CD)?

5. Какие уязвимости существуют в беспроводных сетях на физическом и канальном уровнях?

6. Как защита физических устройств (например, сетевых карт и маршрутизаторов) может повлиять на общую безопасность сети?

7. Что такое атака "перехват канала" и как она может быть предотвращена на физическом уровне?

8. Каковы основные способы защиты от атаки "подавление сигнала" в беспроводных сетях?

9. Какие методы аутентификации и контроля доступа используются для защиты канала связи?

10. Как принципы изоляции и сегментации на физическом и канальном уровнях помогают повышать безопасность сети?

6.1.1 Примеры заданий для практических работ

Тема 3. Безопасность физических и канальных уров-ней сети

Практическое занятие №1. Оценка уязвимостей и методов защиты физических и канальных уровней сети

Цель работы:

Изучить уязвимости, возникающие на физических и канальных уровнях сети, а также оценить методы их защиты.

Задачи:

Оценить уязвимости физической среды передачи данных, включая беспроводные и проводные каналы.

Исследовать методы защиты от атак на физическом уровне (например, перехват сигнала, атаки "подавление сигнала").

Изучить методы обеспечения безопасности на канальном уровне, включая контроль доступа и протоколы аутентификации.

Применить инструменты для тестирования и анализа уязвимостей сети (например, Wireshark для анализа трафика, Aircrack-ng для тестирования безопасности беспроводных сетей).

Провести анализ уязвимостей и предложить меры защиты, используя методы сегментации сети и шифрования на канальном уровне.

Ход работы:

Подготовка лабораторного стенда: Настройте сеть, включая маршрутизаторы, коммутаторы и устройства с возможностью беспроводного подключения.

Оценка уязвимостей: Используйте инструменты для сканирования сети и анализа трафика, чтобы выявить потенциальные угрозы, такие как незащищенные каналы связи или слабые места в аутентификации.

Тестирование защиты: Примените различные методы защиты, включая шифрование на канальном уровне, настройку фильтрации MAC-адресов и настройку WPA2 или WPA3 для защиты беспроводных сетей.

Документирование результатов: Составьте отчет с выводами о найденных уязвимостях, примененных мерах защиты и рекомендациях по улучшению безопасности.

Ожидаемые результаты:

Полученные данные об уязвимостях на физических и канальных уровнях, а также оценка эффективности примененных методов защиты, будут способствовать лучшему пониманию механизмов обеспечения безопасности в реальных сетевых условиях.

Тема 4. Защита периметра и трафика сети

Практическое занятие №2. Настройка и анализ средств защиты периметра и сетевого трафика

Цель работы:

Изучить методы защиты периметра сети и анализа сетевого трафика с целью предотвращения несанкционированных доступов и атак.

Задачи:

Изучить принципы защиты периметра сети с использованием межсетевых экранов (firewall), систем предотвращения вторжений (IPS) и других средств.

Научиться настраивать средства защиты периметра для контроля и фильтрации сетевого трафика.

Применить инструменты для мониторинга и анализа сетевого трафика с целью выявления аномальных действий и возможных угроз.

Оценить эффективность настройки фильтрации трафика, блокировки нежелательных подключений и защиты от атак.

Ознакомиться с методами логирования и отчетности для анализа безопасности сети.

Ход работы:

Подготовка лабораторного стенда: Установите и настройте базовые компоненты сети, включая маршрутизатор, сервер и несколько клиентских машин. Убедитесь, что имеется доступ к интернету или тестовой внешней сети.

Настройка межсетевого экрана (firewall):

Настройте фильтрацию трафика на периметре сети с использованием firewall.

Укажите правила для блокировки нежелательных портов, служб или IP-адресов.

Настройте NAT (Network Address Translation) для скрытия внутренних IP-адресов.

Настройка системы предотвращения вторжений (IPS):

Установите и настройте IPS, чтобы он отслеживал и блокировал подозрительный трафик, например, сканирование портов или попытки эксплуатации уязвимостей.

Примените базовые сигнатуры для защиты от распространенных атак (например, DDoS, SQL-инъекции, и т.д.).

Анализ сетевого трафика:

Используйте инструменты для анализа трафика, такие как Wireshark или tcpdump, чтобы просмотреть и анализировать пакеты данных, проходящие через периметр.

Оцените объем и типы данных, которые проходят через сетевые интерфейсы, и выявите аномалии, такие как несанкционированный доступ или подозрительные соединения.

Проведение атак и тестирование защиты:

Смоделируйте несколько распространенных атак (например, попытки сканирования портов или DDoS-атаку) с использованием инструментов, таких как Nmap или LOIC, и проверьте, как система защиты периметра реагирует на эти угрозы.

Оцените эффективность настроенных фильтров и IPS.

Документирование результатов:

Составьте отчет, в котором будет описано, как были настроены средства защиты, какие атаки были протестированы, какова эффективность защиты и какие рекомендации можно дать для улучшения безопасности.

Ожидаемые результаты:

После выполнения работы студенты должны уметь настроить средства защиты периметра сети, а также проводить анализ сетевого трафика для выявления угроз. Также будет продемонстрирована эффективность различных методов фильтрации и защиты от атак.

Тема 5. Анализ защищённости сети и превентивные механизмы защиты

Практическое занятие №3. Оценка защищённости сети и применение превентивных механизмов защиты

Цель работы:

Изучить методы оценки защищённости сети и применить превентивные механизмы для защиты от угроз и атак.

Задачи:

Оценить уязвимости и риски в сети с использованием инструментов для анализа безопасности.

Изучить принципы и методы превентивной защиты, включая использование антивирусного ПО, систем контроля доступа и шифрования.

Настроить механизмы предотвращения атак и оценить их эффективность.

Использовать инструменты для мониторинга состояния сети и выявления потенциальных угроз.

Разработать рекомендации для повышения уровня безопасности в сети.

Ход работы:

Подготовка лабораторного стенда:

Установите и настройте оборудование, включая маршрутизаторы, коммутаторы и несколько клиентских машин. Убедитесь, что все устройства подключены к сети и доступны для анализа.

Оценка защищённости сети с помощью сканеров уязвимостей:

Используйте инструменты, такие как Nessus или OpenVAS, для сканирования сети на наличие уязвимостей.

Проанализируйте результаты сканирования, чтобы определить слабые места в конфигурации сети и приложений.

Оцените риски, связанные с найденными уязвимостями, и составьте список угроз, которые могут возникнуть в случае эксплуатации этих уязвимостей.

Применение превентивных механизмов защиты:

Установите и настройте антивирусное программное обеспечение на всех устройствах в сети.

Настройте системы контроля доступа, включая использование сильных паролей и многофакторной аутентификации для критичных систем.

Внедрите шифрование данных для защиты конфиденциальной информации при передаче по сети.

Настройка системы мониторинга и обнаружения угроз:

Установите систему мониторинга безопасности (например, SIEM-систему) для отслеживания подозрительных событий в сети.

Настройте уведомления и отчеты для оповещения о возможных атаках или вторжениях.

Проведение тестов на проникновение (Penetration Testing):

Выполните тесты на проникновение с использованием таких инструментов, как Kali Linux или Metasploit, чтобы имитировать действия злоумышленников и проверить эффективность установленных механизмов защиты.

Проанализируйте результаты тестирования, выявите слабые места и предложите способы их устранения.

Документирование результатов:

Составьте отчет, в котором будет отражена оценка защищённости сети, описание применённых превентивных механизмов защиты и результаты тестов на проникновение.

Разработайте рекомендации для улучшения безопасности и повышения устойчивости сети к угрозам.

Ожидаемые результаты:

После выполнения работы студенты должны уметь проводить оценку защищённости сети, использовать инструменты для анализа уязвимостей, настраивать превентивные механизмы защиты, а также выявлять и устранять угрозы с помощью тестирования на проникновение и мониторинга сети.

Тема 6. Угрозы безопасности и встроенные средства защиты операционных систем

Практическое занятие №4. Анализ угроз безопасности и настройка встроенных средств защиты операционных систем

Цель работы:

Изучить угрозы безопасности операционных систем и настроить встроенные средства защиты для предотвращения возможных атак и уязвимостей.

Задачи:

Оценить основные угрозы безопасности для операционных систем.

Изучить встроенные средства защиты операционных систем (антивирусы, файрволы, средства контроля доступа и т.д.).

Настроить и оптимизировать эти средства защиты для повышения уровня безопасности.

Провести анализ угроз, используя средства мониторинга и логирования операционных систем.

Оценить эффективность настроенных средств защиты.

Ход работы:

Подготовка лабораторного стенда:

Установите операционную систему (например, Windows или Linux) на виртуальную или физическую машину. Убедитесь, что система обновлена и готова к настройке встроенных средств защиты.

Анализ угроз безопасности операционных систем:

Проанализируйте типичные угрозы безопасности для операционных систем, включая вредоносные программы (вирусы, трояны, шпионские программы), уязвимости в приложениях и сетевые атаки.

Оцените риски, связанные с несанкционированным доступом, утечкой данных и эксплуатацией уязвимостей.

Настройка встроенных средств защиты (например, на Windows):

Включите и настройте встроенный антивирус (Windows Defender) для регулярной проверки системы.

Настройте брандмауэр Windows для фильтрации входящего и исходящего трафика, создание правил для защиты от атак.

Включите и настройте функции контроля учетных записей (UAC) для ограничения прав пользователей.

Включите шифрование файлов и дисков с помощью BitLocker для защиты конфиденциальных данных.

Для Linux:

Настройте встроенный firewall (например, с помощью iptables или ufw) для фильтрации трафика.

Проверьте и настройте SELinux или AppArmor для повышения безопасности на уровне приложений.

Включите и настройте антивирусное ПО, например ClamAV, для обнаружения вредоносных программ.

Примените методы шифрования данных с помощью инструментов, таких как LUKS (для шифрования дисков).

Мониторинг и анализ угроз:

Используйте встроенные средства логирования и мониторинга операционной системы (например, Event Viewer в Windows или Syslog в Linux) для отслеживания аномальной активности.

Настройте уведомления для подозрительных действий, таких как несанкционированные попытки входа или изменения конфигурации системы.

Проведение тестов на уязвимости и оценка эффективности защиты:

Используйте инструменты для тестирования уязвимостей, например, Nmap или Nessus, чтобы проверить, насколько уязвима система после настройки встроенных средств защиты.

Смоделируйте несколько атак, таких как попытки проникновения через слабые пароли или запуск вредоносного кода, и оцените, как встроенные средства защиты реагируют на эти угрозы.

Документирование результатов:

Составьте отчет, в котором будет подробно описано, какие угрозы безопасности были проанализированы, какие встроенные средства защиты были настроены, а также результаты тестирования и анализа угроз.

Оцените эффективность настроенных средств защиты и предложите рекомендации по дальнейшему улучшению безопасности операционной системы.

Ожидаемые результаты:

После выполнения работы студенты должны уметь анализировать угрозы безопасности для операционных систем, настраивать встроенные средства защиты и оценивать их эффективность через тестирование и мониторинг. Это позволит обеспечить базовую защиту операционной системы от различных угроз.

6.1.3 Перечень вопросов, выносимых на экзамен

1. Что такое компьютерная сеть и какие основные типы сетей существуют?
2. Охарактеризуйте основные принципы построения локальных и глобальных сетей.
3. В чем заключается принцип адресации в компьютерных сетях? Объясните, как работает IP-адресация.
4. Какие функции выполняет модель OSI и как она используется для организации сетевого взаимодействия?
5. Чем отличается коммутация пакетов от коммутации цепей?
6. Каковы основные протоколы канала передачи данных на канальном уровне?
7. Что такое маршрутизация и как она реализуется в компьютерных сетях?
8. В чем заключается роль сетевых устройств, таких как маршрутизаторы, коммутаторы и шлюзы, в обеспечении сетевого взаимодействия?
9. Что такое сетевые уязвимости и как их можно классифицировать?
10. Какие существуют основные виды атак на компьютерные сети и как они классифицируются?
11. Охарактеризуйте атаку "отказ в обслуживании" (DoS) и методы её предотвращения.
12. Что такое атака "человек посередине" (MITM)? Как её можно предотвратить?
13. Какие инструменты можно использовать для сканирования сети на уязвимости?
14. Как работает система обнаружения вторжений (IDS) и какие методы её работы?
15. Что такое уязвимость нулевого дня (zero-day) и чем она опасна для сети?
16. Чем отличаются активные и пассивные методы обнаружения атак в сети?
17. Какие угрозы существуют на физическом уровне сети?
18. Охарактеризуйте атаки на канальный уровень сети, такие как "перехват канала" или "подмена MAC-адресов".
19. Как можно обеспечить безопасность физической среды передачи данных, включая защиту от воздействия электромагнитных излучений?
20. Что такое техника "сканирования сети" и как её можно использовать для анализа уязвимостей канала связи?
21. Какие средства защиты существуют для обеспечения безопасности на канальном уровне (например, фильтрация MAC-адресов)?
22. В чем заключается роль криптографических технологий на канальном уровне для обеспечения безопасности данных?

23. Как защитить беспроводные сети на канальном уровне от перехвата и других атак?

24. Что такое защита периметра сети и какие основные методы защиты существуют?

25. Как работает межсетевой экран (firewall) и какие правила необходимо настроить для защиты сети?

26. Что такое NAT (Network Address Translation) и как он способствует безопасности сети?

27. Какую роль играют системы предотвращения вторжений (IPS) в защите периметра сети?

28. Какие методы используются для защиты трафика сети от атак, таких как eavesdropping или манипуляции с данными?

29. Что такое VPN и как он используется для защиты периметра сети?

30. Какие виды шифрования трафика применяются для защиты данных в процессе передачи?

31. Как настроить защиту от DDoS-атак на уровне периметра сети?

32. Какие методы оценки защищённости сети существуют?

33. Как проводится сканирование на уязвимости в сети с помощью инструментов, таких как Nessus или OpenVAS?

34. Что такое превентивная защита и какие её основные механизмы?

35. Как настроить системы защиты, чтобы предотвратить атаки на уровне сети (например, через фильтрацию и блокировку нежелательных пакетов)?

36. Как применяются технологии шифрования для защиты данных в сети?

37. Как работают системы управления уязвимостями и как они помогают предотвращать угрозы безопасности?

38. Какие принципы защиты важны при построении безопасной сети?

39. Как настроить системы мониторинга и анализа трафика для своевременного обнаружения угроз?

40. Какие угрозы безопасности характерны для операционных систем?

41. Какие встроенные средства защиты существуют в операционных системах (например, антивирусы, фаерволы, контроль доступа)?

42. Как настроить встроенные средства защиты операционной системы для защиты от вирусов и других вредоносных программ?

43. Что такое управление правами доступа и как оно влияет на безопасность операционной системы?

44. Как защитить операционную систему от атак через уязвимости в приложениях?

45. Как работает шифрование данных в операционных системах и какие методы защиты данных на уровне ОС существуют?

46. Что такое контроль целостности системы и как он помогает в обеспечении безопасности?

47. Как встроенные средства защиты операционной системы могут помочь в предотвращении атак, таких как SQL-инъекции или удалённое выполнение кода?

48. Что такое защита от вредоносных программ в операционных системах и как она работает?

6.2 Описание показателей и критериев контроля успеваемости, описание шкал оценивания

Для оценки знаний, умений, навыков и формирования компетенций по дисциплине применяется традиционная система контроля и оценки успеваемости студентов.

При использовании традиционной системы контроля и оценки успеваемости студентов представлены критерии выставления оценок по четырехбалльной системе «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Промежуточный контроль знаний по дисциплине «Интеллектуальный анализ данных» проводится в форме зачета с оценкой. Критерии оценивания результатов обучения представлены в таблице 7.

Таблица 7

Критерии оценивания результатов обучения

Экзамен	Критерии оценивания
Высокий уровень «5» (отлично)	Оценку «**отлично**» заслуживает студент, освоивший знания, умения, компетенции и теоретический материал дисциплины без пробелов; практические навыки профессионального применения освоенных знаний сформированы. Студент самостоятельно и полностью раскрывает сущность теоретических вопросов, использует возможности программных средств для решения прикладных задач; подтверждает ответ конкретными примерами; правильно и обстоятельно отвечает на дополнительные вопросы.
Средний уровень «4» (хорошо)	Оценку **«хорошо»** заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал дисциплины; практические навыки студента в основном сформированы. Студент допускает незначительные ошибки в ответах, самостоятельно использует функции программных средств, подтверждает свои ответы конкретными примерами.
Пороговый уровень «3» (удовлетворительно)	Оценку **«удовлетворительно»** заслуживает студент, частично (с пробелами) освоивший знания, умения, компетенции и теоретический материал дисциплины; некоторые практические навыки студента не сформированы. Студент не может самостоятельно использовать значительную часть функций программных средств, затрудняется подтвердить свои ответы конкретными примерами; неполно отвечает на дополнительные вопросы.
Минимальный уровень «2» (неудовлетворительно)	Оценку **«неудовлетворительно»** заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал дисциплины; практические навыки студента не сформированы. Студент не может использовать программные средства при решении прикладных задач, подтвердить ответы конкретными примерами, не отвечает на дополнительные вопросы преподавателя.

7. Учебно-методическое и информационное обеспечение дисциплины

7.1 Основная литература

1. Лентяева Т. В. Жизненный цикл информационных систем: Практикум: практикум. – Москва: РТУ МИРЭА, 2024. – 74 с. – URL: https://e.lanbook.com/book/432671. – ISBN 978-5-7339-2257-7.
2. Бабенко В. В., Гашин Р. А., Гольчевский Ю. В., Миронов В. В. [и др.] Проектирование, разработка и обеспечение безопасности информационных систем : монография. – Сыктывкар: СГУ им. Питирима Сорокина, 2016. – 146 с. – URL: https://e.lanbook.com/book/176919. – ISBN 978-5-87661-395-0.

7.2 Дополнительная литература

1. Чистов Д. В., Мельников П. П., Золотарюк А. В., Ничепорук Н. Б. Проектирование информационных систем: учебник и практикум для вузов. – Электрон. дан. – Москва: Юрайт, 2021. – 258 с. – (Высшее образование). – URL: https://urait.ru/bcode/469199. – ISBN 978-5-534-00492-2.
2. Токарев В. В., Соколов А. В., Егорова Л. Г., Мышкис П. А. Методы оптимизации. Задачник: учебное пособие для вузов. – Электрон. дан. – Москва: Юрайт, 2024. – 292 с. – (Высшее образование). – URL: https://urait.ru/bcode/541798. – ISBN 978-5-534-10417-2.
3. Золкин А. Л., Мунистер В. Д. Автоматизация и диспетчеризация систем. Применение языковых средств высокоуровневого программирования: учебник для спо. – Санкт-Петербург: Лань, 2025. – 164 с. – URL: https://e.lanbook.com/book/450809. – ISBN 978-5-507-51452-6.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Для освоения материала дисциплины рекомендуется использовать следующие Интернет-ресурсы:

1. . Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [Электронный ресурс]: принят Государственной Думой 8 июля 2006 г. — Режим доступа: [http://pravo.gov.ru]
2. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: принят Государственной Думой 12 июля 2017 г. — Режим доступа: [http://pravo.gov.ru].
3. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» [Электронный ресурс]: принят Государственной Думой 25 марта 2011 г. — Режим доступа: [http://pravo.gov.ru].
4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]: принят Государственной Думой 8 июля 2006 г. — Режим доступа: [http://pravo.gov.ru].
5. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утвер-

ждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

6. ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации в организациях банковской системы Российской Федерации. Общие положения».

7. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

8. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

9. Перечень программного обеспечения

Для чтения лекций по дисциплине «Безопасность и защита информационных систем» требуется аудитория, оснащенная мультимедийным оборудованием.

Для проведения практических занятий требуется сетевой компьютерный класс, оборудованный ПЭВМ с установленным клиентским программным обеспечением из расчета одна ПЭВМ на одного человека. Необходимое программное обеспечение в компьютерном классе перечислено в п. 8.

Таблица 8

Перечень программного обеспечения

№ п/п	Наименование темы учебной дисциплины	Наименование программы	Тип программы	Автор	Год разработки
1	Тема 1-8	Google Chrome	web-браузер	Google	2003 или выше
		Консультант Плюс, Гарант	справочно-правовая	КонсультантПлюс, Гарант	2003 или выше
		MS Office	пакет приложений	Microsoft Corp.	2003 или выше
		Deductor Studio Pro	аналитическая	BaseGroup Labs	2003 или выше

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекции по дисциплине проводятся в специализированной аудитории, оборудованной мультимедийным проектором для демонстрации компьютерных презентаций. Для проведения практических занятий требуется сетевой компьютерный класс, оборудованный ПЭВМ с установленным клиентским

программным обеспечением из расчета, одна ПЭВМ на одного человека. Необходимое программное обеспечение в компьютерном классе перечислено в п. 9 настоящей рабочей программы.

Таблица 9

Сведения об обеспеченности специализированными аудиториями, кабинетами, лабораториями

Наименование специальных помещений и помещений для самостоятельной работы (№ учебного корпуса, № аудитории)	**Оснащенность специальных помещений и помещений для самостоятельной работы**
1	2
Аудитория для проведения занятий лекционного типа, *групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации* (№ 309, уч. корпус № 12)	Видеопроектор и экран для вывода изображения через проектор
Аудитория для проведения практических занятий, *групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации* (№310, уч. корпус №12)	Персональные компьютеры в количестве 24 штук
Аудитория для проведения практических занятий, *групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации* (№315, уч. корпус №12)	Персональные компьютеры в количестве 20 штук
Центральная научная библиотека имени Н.И. Железнова, читальный зал	
Общежитие, комнаты для самоподготовки	

11. Методические рекомендации студентам по освоению дисциплины

Освоение теоретических основ дисциплины предусматривает прослушивание и проработку материала лекций, работу с рекомендованными литературными источниками и Интернет-ресурсами. Лекции читаются в аудиториях, оснащенных мультимедийной техникой, на основе подготовленных презентаций.

Практические навыки по дисциплине приобретаются на практических занятиях. Практические занятия проводятся в компьютерных классах, оснащенных соответствующими техническими и программными средствами. В процессе выполнения заданий практических работ студенты могут обращаться к преподавателю за консультацией по конкретным вопросам.

Самостоятельная работа студентов организуется в соответствии с требованиями п. 4.3 настоящей рабочей программы. Студент обязан в полном объеме использовать предусмотренное время для изучения вопросов, вынесенных на самостоятельное изучение. Во время самостоятельной работы студент прорабатывает материал лекций и обязательной учебной литературы. В

случае возникновения затруднений в освоении материала дисциплины студент обращается к преподавателю за разъяснениями во время, отведенное для индивидуальных консультаций.

Виды и формы отработки пропущенных занятий

Студент, пропустивший занятие лекционного типа, обязан отработать его в одной из следующих форм:

- самостоятельная проработка студентом лекционного материала с использованием рекомендуемой литературы, компьютерных презентаций и конспектов, выполненных другими студентами, с последующим устным опросом;
- реферат на тему, предложенную преподавателем.

При непосещении практического занятия студент обязан его отработать во внеаудиторное время и прийти подготовленным к следующему занятию. Студент самостоятельно прорабатывает материал пропущенного занятия с использованием основной и дополнительной литературы по дисциплине и компьютерных презентаций к лекциям.

12. Методические рекомендации преподавателям по организации обучения по дисциплине

Мультимедийные презентации по дисциплине используются на всех интерактивных лекционных занятиях. Иллюстрационный материал демонстрируется студентам с использованием спецоборудования (мультимедийного проектора) для компьютерных презентаций и программы Microsoft Power Point.

В лекциях рассматриваются только те вопросы, которые не выносятся на самостоятельное изучение. Определенная часть времени лекции выделяется на то, чтобы сориентировать студентов в использовании рекомендуемой литературы и других элементов учебно-методического комплекса дисциплины. Детально рассматриваются основные термины и категории понятийного уровня, что позволяет студентам освоить профессиональную терминологию и легко адаптироваться к реальным условиям производственной, научной и образовательной деятельности.

Практические занятия проводятся в сетевых компьютерных классах, оснащенных соответствующими техническими и программными средствами. Студенты должны быть проинструктированы по технике безопасности работы в компьютерных классах и обязаны выполнять требования инструкций, а также ставить в известность преподавателя и (или) сотрудников УИТ РГАУ-МСХА имени К.А. Тимирязева о фактах нарушения техники безопасности.

Если в процессе выполнения практических работ студент не находит решения стоящих перед ним задач, преподаватель индивидуально консультирует его по конкретным вопросам, связанным с применением изученной методики к конкретному объекту исследования (конкретным данным). Во время практических занятий для целей взаимного обучения разрешается коммуникация между студентами, не выходящая за рамки целей занятия.

При проведении практических занятий следует ориентироваться на современные активные и интерактивные образовательные технологии, основанные на принципах открытости, взаимодействия, активности обучаемых, равенства их аргументов, опоры на групповой опыт, обязательной обратной связи.

Разработчик (и): Пчелинцева С.В., к.т.н., доцент

« 28 » августа 2025 г.

РЕЦЕНЗИЯ

рабочей программы учебной дисциплины Б1.В.03.01 Безопасность и защита информационных систем для подготовки бакалавра по направлению 44.03.04 Профессиональное обучение (по отраслям) направленности «Информационные системы и технологии»

Ашмариной Татьяной Игоревной, доцентом кафедры экономики ФГБОУ ВО РГАУ-МСХА имени К.А. Тимирязева, кандидатом экономических наук (далее по тексту рецензент) проведена рецензия рабочей программы дисциплины «Безопасность и защита информационных систем» ОПОП ВО по направлению 44.03.04 Профессиональное обучение (по отраслям), направленность «Информационные системы и технологии» (бакалавриат), разработанной в ФГБОУ ВО «Российский государственный аграрный университет – МСХА имени К.А. Тимирязева» на кафедре прикладной информатики (разработчик – Пчелинцева С.В., доцент, к.т.н.).

Рассмотрев представленные на рецензию материалы, рецензент пришел к следующим выводам:

1. Предъявленная рабочая программа дисциплины «Безопасность и защита информационных систем» (далее по тексту Программа) *соответствует* требованиям ФГОС ВО по направлению 44.03.04 Профессиональное обучение (по отраслям). Программа *содержит* все основные разделы, *соответствует* требованиям к нормативно-методическим документам.

2. Представленная в Программе ***актуальность*** учебной дисциплины в рамках реализации ОПОП ВО *не подлежит сомнению* – дисциплина относится к обязательной части учебного цикла – Б1.В.

3. Представленные в Программе ***цели*** дисциплины *соответствуют* требованиям ФГОС ВО направления 44.03.04 Профессиональное обучение (по отраслям).

В соответствии с Программой за дисциплиной «Безопасность и защита информационных систем» закреплены одна универсальная и 1 компетенция (3 индикатора) ***компетенций***. Дисциплина «Безопасность и защита информационных систем» и представленная Программа *способна реализовать* их в объявленных требованиях.

4. ***Результаты обучения***, представленные в Программе в категориях знать, уметь, владеть *соответствуют* специфике и содержанию дисциплины и *демонстрируют возможность* получения заявленных результатов.

5. Общая трудоёмкость дисциплины «Безопасность и защита информационных систем» составляет 4 зачётные единицы (108 часов).

6. Информация о взаимосвязи изучаемых дисциплин и вопросам исключения дублирования в содержании дисциплин *соответствует* действительности. Дисциплина «Безопасность и защита информационных систем» взаимосвязана с другими дисциплинами ОПОП ВО и Учебного плана по направлению 44.03.04 Профессиональное обучение (по отраслям) и возможность дублирования в содержании отсутствует.

7. Представленная Программа предполагает использование современных образовательных технологий, используемые при реализации различных видов учебной работы. Формы образовательных технологий *соответствуют* специфике дисциплины.

8. Программа дисциплины «Безопасность и защита информационных систем» предполагает проведение занятий в интерактивной форме.

9. Виды, содержание и трудоёмкость самостоятельной работы студентов, представленные в Программе, *соответствуют* требованиям к подготовке выпускников, содержащимся во ФГОС ВО направления 44.03.04 Профессиональное обучение (по отраслям).

10. Представленные и описанные в Программе формы *текущей* оценки знаний (устный опрос, как в форме обсуждения отдельных вопросов, так и выступления, защита практических работ, защита проектной работы), *соответствуют* специфике дисциплины и требованиям к выпускникам.

Форма промежуточного контроля знаний студентов, предусмотренная Программой, осуществляется в форме зачета, что *соответствует* статусу дисциплины, как дисциплины обязательной части учебного цикла – Б1.О.19 ФГОС ВО направления 44.03.04 Профессиональное обучение (по отраслям)**.**

11. Формы оценки знаний, представленные в Программе, *соответствуют* специфике дисциплины и требованиям к выпускникам.

12. Учебно-методическое обеспечение дисциплины представлено: основной литературой – 5 источника (базовый учебник), дополнительной литературой – 5 наименования, Интернет-ресурсы – 8 источников и *соответствует* требованиям ФГОС ВО направления 44.03.04 Профессиональное обучение (по отраслям)**.**

13. Материально-техническое обеспечение дисциплины соответствует специфике дисциплины «Безопасность и защита информационных систем» и обеспечивает использование современных образовательных, в том числе интерактивных методов обучения.

14. Методические рекомендации студентам и методические рекомендации преподавателям по организации обучения по дисциплине дают представление о специфике обучения по дисциплине «Безопасность и защита информационных систем».

ОБЩИЕ ВЫВОДЫ

На основании проведенной рецензии можно сделать заключение, что характер, структура и содержание рабочей программы дисциплины «Безопасность и защита информационных систем» ОПОП ВО по направлению 44.03.04 Профессиональное обучение (по отраслям), направленность «Информационные системы и технологии» (квалификация выпускника – бакалавр)**,** разработанной Пчелинцевой С.В., доцентом кафедры прикладной информатики, соответствует требованиям ФГОС ВО, современным требованиям экономики, рынка труда и позволит при её реализации успешно обеспечить формирование заявленных компетенций.

Рецензент: Ашмарина Т.И., к.э.н, доцент _____
(ФИО, ученая степень, ученое звание) (подпись)

« 28 » августа 2025 г.