

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Узунов Федор Владимирович

Должность: Ректор

Дата подписания: 30.09.2026 09:20:02

Уникальный программный ключ:

fd935d10451b860e912264c0378f8448452b603f94388008e29877a6bcbf5

**АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
«ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ»**

«УНИВЕРСИТЕТ ЭКОНОМИКИ И УПРАВЛЕНИЯ»

Факультет экономики, управления и юриспруденции

Кафедра «Управление и бизнес-информатика»



УТВЕРЖДАЮ

Проректор по учебно-методической работе

[Signature] / Г.П. Узунова

«02» февраля 2026 г.

Рабочая программа дисциплины

Программно-аппаратные средства защиты информации

Направление подготовки

10.03.01 «Информационная безопасность»

Профиль

Безопасность компьютерных систем

Квалификация выпускника

Бакалавр

Для всех

форм обучения

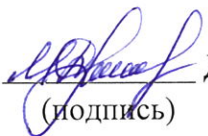
Симферополь, 2026

Рабочая программа составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки 10.03.01 «Информационная безопасность» профиль Безопасность компьютерных систем, утвержденным приказом Министерства образования и науки Российской Федерации от 17.11.2020 г. № 1427 (зарегистрировано в Министерстве юстиции РФ 18.02.2021 №62548) с изменениями и дополнениями.

Программу составил Фурин А.Д., преподаватель

Рабочая программа дисциплины «Программно-аппаратные средства защиты информации» утверждена на заседании кафедры «Управление и бизнес-информатика».

Протокол № 6 от 29.01.2026 г.

Заведующий кафедрой  Д.В. Моторина
(подпись)

АННОТАЦИЯ	
Индекс дисциплины по учебному плану	Наименование дисциплины
Б1.О.22	ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ
Цель изучения дисциплины	сформировать знания в области информационных технологий, выработать необходимые умения и навыки использования современных аппаратных и программных средств сбора, представления, хранения, передачи, обработки, анализа данных в профессиональной деятельности.
Место дисциплины в структуре ОПОП	Дисциплина «Основы управления информационной безопасностью» является дисциплиной базовой части программы учебного плана
Компетенции, формируемые в результате освоения дисциплины	ОПК-10
Содержание дисциплины	Введение. Тема 1 Задачи и принципы организации службы информационной безопасности Тема 2 Создание службы информационной безопасности. Тема 3 Требования к сотрудникам СИБ. Тема 4 Инвентаризация информационных систем Тема 5 Классификация информационных систем Тема 6 Классификация объектов и субъектов информационных отношений Тема 7 Оценка информационных рисков. Тема 8 Управление информационными рисками. Тема 9 Работа службы информационной безопасности с оборудованием информационных систем. Тема 10 Работа службы Информационной безопасности с персоналом. Тема 11 Создание политики информационной безопасности. Тема 12 Создание механизмов информационной безопасности и их тестирование. Тема 13 Создание аварийного плана. Тема 14 Состав и содержание документов. Тема 15 Работа службы Информационной безопасности с аварийным планом. Тема 16 Работа службы информационной безопасности при нарушении правил защиты информации
Общая трудоемкость дисциплины	Общая трудоемкость дисциплины составляет 6 зачетных единиц (144часов)
Форма промежуточной аттестации	Зачет с оценкой

Содержание

1. Цель и перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы бакалавриата	5
2. Место дисциплины в структуре ОПОП бакалавриата	5
3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся	5
4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий	6
5. Контроль качества освоения дисциплины	11
6. Учебно-методическое обеспечение дисциплины	11
7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	11
8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	12
9. Методические указания для обучающихся по освоению дисциплины	13
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)	13
11. Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине	14
Приложение к РПД	15

1. Цель и перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы бакалавриата

Цель изучения дисциплины «Программно-аппаратные средства защиты информации» – сформировать знания в области информационных технологий, выработать необходимые умения и навыки использования современных аппаратных и программных средств сбора, представления, хранения, передачи, обработки, анализа данных в профессиональной деятельности.

В результате освоения ОПОП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине:

Код компетенции	Результаты освоения ОПОП (содержание компетенций)	Планируемые результаты освоения дисциплины
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.1. Выбирает принципы формирования политики информационной безопасности в информационных системах ОПК-10.2. Подбирает и конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина «Программно-аппаратные средства защиты информации» относится к базовой части учебного плана и изучается на 2 курсе в 4 семестре по очной форме обучения.

Для изучения дисциплины студент должен:

- знать основы математических и информационных технологий, виды программного обеспечения;
- уметь пользоваться базовым программным и математическим обеспечением.

Для успешного освоения дисциплины «Программно-аппаратные средства защиты информации» студент должен изучить курс «Организационное и правовое обеспечение информационной безопасности».

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

Общая трудоемкость (объем) дисциплины составляет 4 зачетных единицы (з.е.), 144 академических часа.

3.1. Объём дисциплины по видам учебных занятий (в часах)

Для очной формы обучения

Общая трудоёмкость дисциплины составляет 4 зачётных единицы 144 часа

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	144

Контактная работа	44
Аудиторная работа (всего):	44
Лекции	28
Семинары, практические занятия	16
Самостоятельная работа обучающихся (всего)	100
Курсовая работа	-
Зачет	+
Экзамен	-

Для очно-заочной формы обучения

Общая трудоёмкость дисциплины составляет 4 зачётных единицы 144 часа

Объём дисциплины	Всего часов
Общая трудоёмкость дисциплины	144
Контактная работа	28
Аудиторная работа (всего):	28
Лекции	10
Семинары, практические занятия	18
Самостоятельная работа обучающихся (всего)	106
Курсовая работа	-
Зачет	+
Экзамен	-

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

4.1. Разделы дисциплины и трудоёмкость по видам учебных занятий (в академических часах)

№ темы	Наименование темы	Всего		Количество часов					
		ОФО	ОЗФО	Контактная работа				Внеаудит. работа	
				Лекции		Практические		Самост. работа	
				ОФО	ОЗФО	ОФО	ОЗФО	ОФО	ОЗФО
1.	Компьютерная система и защита информации	11	11	2	2	1	1	8	8
2.	Методы защиты информации	11	11	2	2	1	1	8	8
3.	Общая характеристика существующих средств защиты информации от несанкционированного доступа	11	11	2	2	1	1	8	8
4	Общие сведения об антивирусных	11	11	2	2	1	1	8	8

	программах								
5	Функции антивирусного программного обеспечения и уровни защиты от компьютерных вирусов	11	11	2	2	1	1	8	8
6	Понятие межсетевого экрана	11	9	2	-	1	1	8	8
7	Основные компоненты межсетевых экранов	11	9	2	-	1	1	8	8
8	Обход межсетевых экранов	11	9	2	-	1	1	8	8
9	Защита программных продуктов от несанкционированного копирования	11	9	2	-	1	1	8	8
10	Защита программных продуктов от исследования	11	9	2	-	1	1	8	8
11	Модели и классификация систем обнаружения вторжений.	8	8	2	-	1	2	6	6
12	Обнаружения аномалий	9	8	2		1	2	6	6
13	Методы обхода систем обнаружения вторжений	10	6	2	-	2	2	6	6
14	Тестирование систем обнаружения вторжений	6	8	2		2	2	2	8
	Всего по дисциплине	144	144	28	10	16	18	100	106
	Контроль	-	-						
	Итого	144	144	28	10	16	18	100	106

4.2. Содержание дисциплины, структурированное по темам (разделам)

Введение

Предмет и задачи дисциплины. Рекомендуемая литература. Краткий обзор развития теории управления ИБ

Тема 1. Компьютерная система и защита информации

Основные понятия и определения. Нормативные и правовые документы по защите информации от несанкционированного доступа. Требования по защите информации от несанкционированного доступа.

Тема 2. Методы защиты информации

Идентификация и аутентификация пользователей. Ограничение доступа на вход в систему. Разграничение доступа. Регистрация событий (аудит). Криптографическая защита. Контроль целостности. Управление политикой безопасности. Уничтожение остаточной информации. Комплексный подход к защите.

Тема 3. Общая характеристика существующих средств защиты информации от несанкционированного доступа

Средства защиты информации от несанкционированного доступа. Средства криптографической защиты информации.

Тема 4. Общие сведения об антивирусных программах

История создания антивирусных программ. Целевые платформы антивирусного программного обеспечения. Классификация антивирусных продуктов.

Тема 5 Функции антивирусного программного обеспечения и уровни защиты от компьютерных вирусов

Функции антивирусов. Защита от проникновения вирусов известных типов. Углублённый анализ на наличие вирусов. Защита от деструктивных действий и размножения вирусов.

Тема 6 Понятие межсетевого экрана

Понятие межсетевого экрана. Положительные и Отрицательные стороны применения межсетевых экранов. Требования к показателям защищенности межсетевых экранов.

Тема 7 Основные компоненты межсетевых экранов

Фильтрация пакетов. Межсетевые экраны уровня соединения. Межсетевые экраны прикладного уровня. Межсетевые экраны с динамической фильтрацией пакетов. Межсетевые экраны инспекции состояния. Межсетевые экраны уровня ядра.

Тема 8 Обход межсетевых экранов.

Постепенный подход. Туннелирование.

Тема 9 Защита программных продуктов от несанкционированного копирования

Методы, затрудняющие считывание скопированной информации. Методы, препятствующие использованию скопированной информации. Основные функции средств защиты от копирования. Основные методы защиты от копирования. Методы противодействия динамическим способам снятия защиты от копирования.

Тема 10 Защита программных продуктов от исследования.

Классификация средств исследования программ. Методы защиты программ от исследования.

Тема 11 Модели и классификация систем обнаружения вторжений

Модель Д.Деннинг. Модель CIDF. Классификация систем обнаружения вторжений. Обнаружение сигнатур.

Тема 12 Обнаружения аномалий.

Методы Data Mining. Методы технологий мобильных агентов. Методы построения иммунных систем. Применение Генетических алгоритмов. Применение нейронных сетей. Языки описания атак.

Тема 13 Методы обхода систем обнаружения вторжений.

Методы обхода сетевых систем обнаружения вторжений. Методы обхода хостовых систем обнаружения вторжений.

Тема 14. Тестирование систем обнаружения вторжений

Тестирование коммерческих систем. Тестирование исследовательских прототипов.

4.3. Содержание практических занятий (очная форма обучения)

Тема 9. Средства защиты информации от несанкционированного доступа (8 часов) <i>Лабораторная работа №01.</i> <i>«Установка и настройка СЗИ от НСД: «Dallas Lock 7», «Secret Net 5», «Аура».»</i>
Тема 4. Антивирусные средства. (6 часов) <i>Лабораторная работа №02.</i> <i>«Изучение, анализ и настройка антивирусного программного обеспечения: Dr.Web.»</i>
Тема 6 Межсетевые экраны. (8 часов) <i>Лабораторная работа №03.</i> <i>«Инсталляция и настройка межсетевых экранов: CheckPoint.»</i>
Тема 10 Защита программных продуктов. (6 часов) <i>Лабораторная работа №04.</i> <i>«Изучение работы средств защиты программных продуктов.»</i>
Тема 12 Системы обнаружения атак и вторжений. <i>Лабораторная работа №05.</i> <i>«Изучение работы средств обнаружения вторжений.»</i>

4.4. Содержание самостоятельной работы

№ п/п	Вид самостоятельной работы	Наименование работы и содержание
1	Реферат	Применение антивирусного средства для защиты информации
2	Самостоятельное изучение онлайн-курса	Онлайн-курс «Программно аппаратные средства защиты информации» https://farvater.gumrf.ru/course/view .

5. Контроль качества освоения дисциплины

Текущий контроль и промежуточная аттестация осуществляются в соответствии с «Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся в Автономной некоммерческой организации «Образовательная организация высшего образования» «Университет экономики и управления».

Вид промежуточной аттестации – зачет с оценкой. Форма проведения промежуточной аттестации – письменный зачет.

Фонд оценочных средств по дисциплине приведен в приложении к РПД.

6. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) основная литература:

1. Программно-аппаратные средства защиты информации : учебное пособие / С. А. Зырянов, М. А. Кувшинов, И. А. Огнев, И. В. Никрошкин. — Новосибирск : Новосибирский государственный технический университет, 2023. — 80 с. — ISBN 978-5-7782-4905-9. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/155427/details> (дата обращения: 27.01.2026). — Режим доступа: для авторизир. пользователей

2. Программно-аппаратные средства защиты информации. В 3 частях. Ч.3 : учебное пособие / В. А. Гриднев, Ю. А. Губсков, А. С. Дерябин, А. В. Яковлев. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2024. — 81 с. — ISBN 978-5-8265-2795-5. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/145338/details> (дата обращения: 27.01.2026). — Режим доступа: для авторизир. пользователей

б) дополнительная литература:

3. Программно-аппаратные средства защиты информации. В 3 частях. Ч.2 : учебное пособие / В. А. Гриднев, Ю. А. Губсков, А. С. Дерябин, А. В. Яковлев. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2023. — 79 с. — ISBN 978-5-8265-2464-0, 978-5-8265-2609-5 (ч.2). — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/141077/details> (дата обращения: 27.01.2026). — Режим доступа: для авторизир. пользователей

4. Солонская, О. И. Средства защиты информации : учебное пособие для СПО / О. И. Солонская. — Саратов : Профобразование, 2022. — 88 с. — ISBN 978-5-4488-1504-1. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/125578/details> (дата обращения: 27.01.2026). — DOI: <https://doi.org/10.23682/125578>. — Режим доступа: для авторизир. пользователей

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

1. Информационно-правовой портал «Гарант»: официальный сайт. — URL: <http://www.garant.ru> — Текст: электронный.

2. Цифровой образовательный ресурс «IPRsmart»: официальный сайт. — URL: <http://www.iprbookshop.ru/> — Текст: электронный.

3. Научная электронная библиотека «КиберЛенинка»: официальный сайт. — URL: <https://cyberleninka.ru/> — Текст: электронный.

4. Российский интернет-портал и аналитическое агентство TAdviser: официальный сайт. — URL: <https://www.tadviser.ru/> — Текст: электронный.

8. Методические указания для обучающихся по освоению дисциплины

При проведении лекций, семинарских (практических) занятий, самостоятельной работе обучающихся применяются интерактивные формы проведения занятий с целью погружения обучающихся в реальную атмосферу профессионального сотрудничества по разрешению проблем, оптимальной выработки навыков и качеств будущего специалиста. Интерактивные формы проведения занятий предполагают обучение в сотрудничестве. Все участники образовательного процесса (преподаватель и обучающиеся) взаимодействуют друг с другом, обмениваются информацией, совместно решают проблемы, моделируют ситуацию.

В учебном процессе используются интерактивные формы занятий:

- творческое задание. Выполнение творческих заданий требует от обучающегося воспроизведение полученной ранее информации в форме, определяемой преподавателем, и требующей творческого подхода;

- групповое обсуждение. Групповое обсуждение кого-либо вопроса направлено на достижение лучшего взаимопонимания и способствует лучшему усвоению изучаемого материала.

В ходе освоения дисциплины при проведении контактных занятий используются следующие формы обучения, способствующие формированию компетенций: лекции-дискуссии; кейс-метод; решение задач; ситуационный анализ; обсуждение рефератов и докладов; разработка групповых проектов; встречи с представителями государственных и общественных организаций.

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

В процессе лекционных и практических занятий используется следующее программное обеспечение:

- *программы, обеспечивающие доступ в сеть «Интернет» (например, «Microsoft Edge», «Google Chrome»);
- *программы, демонстрации видео материалов (например, проигрыватель «Windows Media Player»);
- *текстовые редакторы и процессоры (например, «Microsoft Office Word»);
- *табличные процессоры (например, «Microsoft Office Excel»);
- *системы управления базами данных (например, «Microsoft Office Access»);
- *программы для демонстрации и создания презентаций (например, «Microsoft PowerPoint»);
- *проблемно-ориентированные пакеты прикладных программ по отраслям и сферам деятельности (например, «1С: Управление нашей фирмой», «Loginom Community Edition»).

10. Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине

Учебная аудитория

Оборудование учебной аудитории:

рабочее место преподавателя ; посадочные места по количеству обучающихся ;
доска классная ;
стенды информационные ;

Учебно-наглядные пособия: компьютеры с лицензионным программным обеспечением и возможностью подключения к информационно-телекоммуникационной сети Интернет ; мультимедийная установка .

Помещение для самостоятельной работы обучающихся

оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета.