

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Узунов Федор Владимирович

Должность: Ректор

Дата подписания: 30.09.2026 09:20:01

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

Г.П. Узунова / Г.П. Узунова

«02» февраля 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита операционных систем устройств

Направление подготовки

09.03.01 «Информатика и вычислительная техника»

Профиль

Специалист по информационным системам

Квалификация выпускника

Бакалавр

Для всех

форм обучения

Симферополь, 2026

Рабочая программа составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки 09.03.01 "Информатика и вычислительная техника", утвержденного приказом Министерства науки и высшего образования Российской Федерации от 19.09.2017 №929 (зарегистрировано в Министерстве юстиции РФ 10.10.2017 №48489) с изменениями и дополнениями.

Программу составил Яковенко Л.В., преподаватель

Рабочая программа дисциплины «Защита операционных систем устройств» 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.В.ДВ.04.01	Защита операционных систем устройств
Цель изучения дисциплины	формирование у студентов профессиональных компетенций, необходимых для обеспечения безопасности программно-аппаратных платформ на уровне ядра и системного окружения. Дисциплина направлена на изучение архитектуры подсистем защиты современных ОС (Windows, Linux, macOS), методов противодействия несанкционированному доступу к ресурсам и принципов администрирования политик безопасности.
Место дисциплины в структуре ОПОП	Дисциплина Операционные системы относится к базовой части ОПОП, формируемой участниками образовательных отношений.
Компетенции, формируемые в результате освоения дисциплины	ПК-1
Содержание дисциплины	Тема 1. Архитектура защищенных ОС и модель разграничения доступа (DAC/MAC). Тема 2. Механизмы идентификации, аутентификации и авторизации. Тема 3. Управление учетными записями, ролями и делегирование полномочий. Тема 4. Подсистема аудита событий безопасности и мониторинг целостности. Тема 5. Безопасность ядра, драйверов и защита от выполнения данных (DEP/NX). Тема 6. Изоляция сред исполнения: песочницы, контейнеры и виртуализация.
Общая трудоемкость дисциплины	Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часов)
Форма промежуточной аттестации	Экзамен

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. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	11
7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	12
8. Методические указания для обучающихся по освоению дисциплины	13
9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)	13
10. Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине	14

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

Цель изучения дисциплины «Защита операционных систем устройств» – формирование у студентов профессиональных компетенций, необходимых для обеспечения безопасности программно-аппаратных платформ на уровне ядра и системного окружения. Дисциплина направлена на изучение архитектуры подсистем защиты современных ОС (Windows, Linux, macOS), методов противодействия несанкционированному доступу к ресурсам и принципов администрирования политик безопасности.

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

Коды компетенции	Результаты Освоения ОПОП	Перечень планируемых результатов обучения по дисциплине
ПК-1	Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1.1. Знает современные виды информационного взаимодействия и обслуживания, принципы и методы противодействия несанкционированному воздействию на вычислительные сети и системы передачи информации, основные задачи и понятия криптографии, требования к шифрам и основные характеристики шифров, модели шифров и математические методы их исследования, принципы построения криптографических алгоритмов. ПК-1.2. Умеет использовать и настраивать программно-аппаратные средства защиты информации, проводить анализ показателей качества сетей и систем связи ПК-1.3. Владеет навыками по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина Защита операционных систем устройств относится к базовой части ОПОП и является обязательной для освоения, изучается обучающимися очной формы обучения в 8 семестре, очно-заочной формы обучения – в 8 семестре.

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 трудоёмкость дисциплины	144
Контактная работа	44
Аудиторная работа (всего):	44
Лекции	28
Семинары, практические занятия	16
Самостоятельная работа обучающихся (всего)	72
Экзамен	36

Для очно-заочной формы обучения

Общая трудоёмкость дисциплины составляет 4 зачётных единицы 144 часа

Объём дисциплины	Всего часов
Общая трудоёмкость дисциплины	144
Контактная работа	34
Аудиторная работа (всего):	34
Лекции	22
Семинары, практические занятия	12
Самостоятельная работа обучающихся (всего)	82
Экзамен	36

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.	Тема 1. Архитектура защищенных ОС и модель разграничения доступа (DAC/MAC).	22	22	4	2	2	2	16	18
2.	Тема 2. Механизмы идентификации, аутентификации и авторизации.	22	26	4	4	2	2	16	20

3.	Тема 3. Управление учетными записями, ролями и делегирование полномочий.	22	24	4	4	2	4	16	18
4.	Тема 4. Подсистема аудита событий безопасности и мониторинг целостности.	24	24	4	4	2	2	16	18
5.	Тема 5. Безопасность ядра, драйверов и защита от выполнения данных (DEP/NX).	26	24	6	4	4	2	18	18
6.	Тема 6. Изоляция сред исполнения: песочницы, контейнеры и виртуализация.	26	24	6	4	4	2	18	18
	Всего по дисциплине	108	108	28	22	16	12	72	82
	Контроль	36	36						
	Итого	144	144						

4.2. Содержание дисциплины, структурированное по темам (разделам)

Тема 1. Архитектура защищенных ОС и модель разграничения доступа (DAC/MAC) Раскрывается отличие классических дискреционных моделей (*Discretionary Access Control* — права владельца файла) от принудительных мандатных моделей (*Mandatory Access Control*). Изучаются реализации MAC в отечественных ОС (МРОСЛ ДП-модели в Astra Linux SELinux в RHEL/CentOS). Рассматривается концепция субъектов (процессы, пользователи) и объектов (файлы, порты, память).

Тема 2. Механизмы идентификации, аутентификации и авторизации Изучается процесс проверки подлинности пользователя: от ввода пароля до создания токена доступа (*Access Token*) или процесса-демона с правами UID=0 (root). Анализируются методы безопасного хранения хешей паролей (/etc/shadow, SAM-база Windows), использование аппаратных модулей безопасности (TPM, смарт-карты) и протоколов сквозной аутентификации (*Kerberos*).

Тема 3. Управление учетными записями, ролями и делегирование полномочий Рассматриваются принципы минимальных привилегий. Изучается архитектура повышения прав (UAC в Windows, sudo в Unix-подобных системах). Разбирается построение ролевых моделей доступа (RBAC) для разделения обязанностей администратора сети, аудитора и обычного пользователя, чтобы исключить наличие постоянных суперпользовательских сессий.

Тема 4. Подсистема аудита событий безопасности и мониторинг целостности Анализируется работа служб регистрации событий (*Event Viewer* в Windows, *auditd* в Linux). Изучается настройка правил фиксации критических действий: вход в систему, изменение прав доступа на файлы, запуск процессов. Рассматривается контроль целостности системных файлов (например, механизм *AIDE* или встроенный *Windows Resource Protection*) для обнаружения внедрения руткитов.

Тема 5. Безопасность ядра, драйверов и защита от выполнения данных (DEP/NX) Раскрываются низкоуровневые механизмы защиты. Изучается технология предотвращения выполнения данных (*DEP / NX-bit*), блокирующая исполнение кода из областей памяти, помеченных как данные. Рассматривается рандомизация размещения

адресного пространства (ASLR) для затруднения эксплуатации уязвимостей переполнения буфера. Анализируются риски установки недоверенных драйверов уровня ядра.

Тема 6. Изоляция сред исполнения: песочницы, контейнеры и виртуализация
Рассматриваются современные методы ограничения воздействия вредоносного ПО. Изучается архитектура «песочниц» приложений (*AppContainer* в Windows, *Seatbelt* в macOS), механизмов изоляции процессов через пространства имен (*namespaces*) и контрольные группы (*cgroups*) в Linux (основа Docker), а также гипервизоров первого и второго типа для полной изоляции гостевых операционных систем друг от друга и от хост-платформы.

4.3. Содержание практических занятий (очная форма обучения)

Разделы, темы, дидактические единицы
Тема 1. Архитектура защищенных ОС и модель разграничения доступа (DAC/MAC) Раскрывается отличие классических дискреционных моделей (<i>Discretionary Access Control</i> — права владельца файла) от принудительных мандатных моделей (<i>Mandatory Access Control</i>).
Тема 2. Механизмы идентификации, аутентификации и авторизации Изучается процесс проверки подлинности пользователя: от ввода пароля до создания токена доступа (<i>Access Token</i>) или процесса-демона с правами <i>UID=0</i> (<i>root</i>).
Тема 3. Управление учетными записями, ролями и делегирование полномочий Рассматриваются принципы минимальных привилегий. Изучается архитектура повышения прав (<i>UAC</i> в Windows, <i>sudo</i> в Unix-подобных системах).
Тема 4. Подсистема аудита событий безопасности и мониторинг целостности Анализируется работа служб регистрации событий (<i>Event Viewer</i> в Windows, <i>auditd</i> в Linux). Изучается настройка правил фиксации критических действий: вход в систему, изменение прав доступа на файлы, запуск процессов.
Тема 5. Безопасность ядра, драйверов и защита от выполнения данных (DEP/NX) Раскрываются низкоуровневые механизмы защиты. Изучается технология предотвращения выполнения данных (<i>DEP / NX-bit</i>), блокирующая исполнение кода из областей памяти, помеченных как данные.
Тема 6. Изоляция сред исполнения: песочницы, контейнеры и виртуализация Рассматриваются современные методы ограничения воздействия вредоносного ПО. Изучается архитектура «песочниц» приложений (<i>AppContainer</i> в Windows, <i>Seatbelt</i> в macOS), механизмов изоляции процессов через пространства имен (<i>namespaces</i>).

4.4. Содержание самостоятельной работы

Разделы, темы, дидактические единицы
Тема 1. Архитектура защищенных ОС и модель разграничения доступа (DAC/MAC) Рассматривается концепция субъектов (процессы, пользователи) и объектов (файлы, порты, память).
Тема 2. Механизмы идентификации, аутентификации и авторизации Методы безопасного хранения хешей паролей (<i>/etc/shadow</i> , <i>SAM</i> -база Windows), использование аппаратных модулей безопасности (<i>TPM</i> , смарт-карты) и протоколов сквозной аутентификации (<i>Kerberos</i>).
Тема 3. Управление учетными записями, ролями и делегирование полномочий Построение ролевых моделей доступа (<i>RBAC</i>) для разделения обязанностей администратора сети, аудитора и обычного пользователя, чтобы исключить наличие постоянных суперпользовательских сессий.

Тема 4. Подсистема аудита событий безопасности и мониторинг целостности Контроль целостности системных файлов (например, механизм <i>AIDE</i> или встроенный <i>Windows Resource Protection</i>) для обнаружения внедрения руткитов.
Тема 5. Безопасность ядра, драйверов и защита от выполнения данных (DEP/NX) Рандомизация размещения адресного пространства (<i>ASLR</i>) для затруднения эксплуатации уязвимостей переполнения буфера. Анализируются риски установки недоверенных драйверов уровня ядра.
Тема 6. Изоляция сред исполнения: песочницы, контейнеры и виртуализация Контрольные группы (<i>cgroups</i>) в Linux (основа <i>Docker</i>), а также гипервизоров первого и второго типа для полной изоляции гостевых операционных систем друг от друга и от хост-платформы.

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. 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. Гарькушев, А. Ю. Основы обеспечения безопасности операционных систем : учебное пособие / А. Ю. Гарькушев, А. В. Липис, И. Л. Карпова. — Москва, Вологда : Инфра-Инженерия, 2024. — 124 с. — ISBN 978-5-9729-1851-5. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/143546/details> (дата обращения: 27.01.2026). — Режим доступа: для авторизир. пользователей

2. Моргунов А.В. Операционные системы : учебное пособие / Моргунов А.В.. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2024. — 72 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/149525.html> (дата обращения: 04.05.2025). — Режим доступа: для авторизир. пользователей

б) дополнительная литература:

3. Шапошников А.В. Операционные системы : учебное пособие (лабораторный практикум) / Шапошников А.В., Ляхов П.А., Ионисян А.С.. — Ставрополь : Северо-Кавказский федеральный университет, 2022. — 143 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/135709.html> (дата обращения: 04.05.2025). — 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