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
«02» февраля 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Компьютерные вирусы

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 «Компьютерные вирусы» 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.10	Компьютерные вирусы
Цель изучения дисциплины	формирование у обучающихся знаний и навыков в области компьютерной вирусологии, а также на подготовку к организации эффективной защиты компьютерных систем и сетей от вредоносного программного обеспечения.
Место дисциплины в структуре ОПОП	Дисциплина относится к части, формируемой участниками образовательных отношений блока 1 программы бакалавриата.
Компетенции, формируемые в результате освоения дисциплины	ПК-4
Содержание дисциплины	Тема 1. Введение в компьютерную вирусологию Тема 2. Основные признаки присутствия вредоносных программ и методы по устранению последствий вирусных заражений Тема 3. Установка Kaspersky для Linux. Тема 4. ЗАРАЖЕНИЕ EXE-файлов Тема 5. Файловые вирусы Тема 6. Методы защиты от программ деструктивного воздействия Тема 7. «Защита серверов и рабочих станций
Общая трудоемкость дисциплины	Общая трудоемкость дисциплины составляет 4 зачетных единицы (144 часа)
Форма промежуточной аттестации	Зачет с оценкой

Содержание

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

Цель изучения дисциплины «Компьютерные вирусы» – формирование у обучающихся знаний и навыков в области компьютерной вирусологии, а также на подготовку к организации эффективной защиты компьютерных систем и сетей от вредоносного программного обеспечения.

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-4	Способен разрабатывать, внедрять и адаптировать прикладное программное обеспечение	ПК-4.1. Знать: программные шаблоны; метрики и риски тестирования; базовые понятия качества программного продукта и качества процесса разработки программного обеспечения; основные концепции и атрибуты качества программного обеспечения (надежности, безопасности, удобства использования); функциональные характеристики применения программного обеспечения. ПК-4.2. Уметь: реализовывать программные продукты на языках программирования высокого уровня; описывать архитектуру программного средства включая выделение: функциональных компонентов и модулей, структур данных, внешних и внутренних интерфейсов; применять соответствующие программные или аппаратные архитектурные решения; использовать модели данных; анализировать и оценивать архитектуру на предмет атрибутов качества. ПК-4.3. Владеть: навыками планирования процесса разработки программного продукта; навыками задания функциональных рамок подсистем; навыками определения наиболее значимых критериев качества программного продукта

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина Б1.В.10 «Компьютерные вирусы» относится к части, формируемой участниками образовательных отношений блока 1 учебного плана ОПОП бакалавриата по направлению подготовки 09.03.01 Информатика и вычислительная техника. Дисциплина «Компьютерные вирусы» изучается обучающимися очной формы обучения во 8 семестре, очно-заочной формы обучения – во 9 семестре.

При изучении данной дисциплины обучающийся использует знания, умения и навыки, которые сформированы в процессе изучения предшествующих дисциплин: «Линейная алгебра и геометрия», «Информационные технологии в профессиональной деятельности» и др.

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	22
Семинары, практические занятия	22
Самостоятельная работа обучающихся (всего)	100
Зачет с оценкой	+

Для очно-заочной формы обучения

Общая трудоёмкость дисциплины составляет 4 зачётных единицы 144 часа

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	144
Контактная работа	34
Аудиторная работа (всего):	34
Лекции	16
Семинары, практические занятия	18
Самостоятельная работа обучающихся (всего)	110
Зачет с оценкой	+

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

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

№ темы	Наименование темы	Всего		Количество часов					
				Контактная работа				Внеаудит. работа	
				Лекции		Практические		Самост. работа	
		ОФО	ОЗФО	ОФО	ОЗФО	ОФО	ОЗФО	ОФО	ОЗФО

1.	Тема 1. Введение в компьютерную вирусологию	18	18	2	2	2	2	14	14
2.	Тема 2. Основные признаки присутствия вредоносных программ и методы по устранению последствий вирусных заражений	18	18	4	2	2	2	12	14
3.	Тема 3. Установка Kaspersky для Linux.	18	18	4	2	4	2	10	14
4.	Тема 4. ЗАРАЖЕНИЕ EXE-файлов	18	18	4	2	4	2	10	14
5.	Тема 5. Файловые вирусы	18	18	4	4	4	4	10	10
6.	Тема 6. Методы защиты от программ деструктивного воздействия	36	36	2	2	4	4	30	30
7.	Тема 7. «Защита серверов и рабочих станций	18	18	2	2	2	2	14	14
	Всего по дисциплине	**144**	**144**	**22**	**16**	**22**	**18**	**100**	**110**
	Контроль	-	-						
	Итого	**144**	**144**						

4.2. Содержание дисциплины, структурированное по темам (разделам)

Тема 1. Введение в компьютерную вирусологию

Появление термина «Компьютерный вирус», военные разработки, возникновение эпидемий компьютерных вирусов. Результат Фреда Коэна. Результат Д. Чесса и С. Вайта. Формализм Ф. Лейтольда. Результат Леонарда Адельмана.

Определение компьютерного вируса. Отличительные особенности компьютерных вирусов и других вредоносных программ. Классификация по способу использования ресурсов. Класси-фикация по типу заражаемых объектов. Классификация по принципам активации. Классификация по способу организации программного кода. Классификация по вредоносным функциям. Классификация по степени опасности

Тема 2. Основные признаки присутствия вредоносных программ и методы по устранению последствий вирусных заражений

Использование Диспетчера задач ОС для анализа подозрительных процессов. Анализ статистку текущих сетевых подключений компьютера с параметрами подключений портов.

Установка ClamAV. Настройка обновления. Сканирование системы с помощью ClamAV.Установка ClamTk (графический пользовательский интерфейс для ClamAV) / База знаний РЕД ОС.

Изучение структуры файла программы вируса, способов её загрузки и воздействия на COM-файлы на примере тестовой программы вируса. Его обнаружение и нейтрализация с помощью антивирусного комплекса.

Загрузка с винчестера. Как устроены загрузочные вирусы. Как загрузочные вирусы получают управление. Как загрузочные вирусы заражают свои жертвы. Как вирусы остаются резидентно в памяти

Тема 3. Установка Kaspersky для Linux.

Изучение руководства по использованию. Инсталяция дистрибутива программы. Установка Агента администрирования. Начальная настройка параметров Агента администрирования. Тестирование программы. / ПО Лаборатории Касперского. РЭД ОС LibreOffice

Тема 4. ЗАРАЖЕНИЕ EXE-файлов

Изучение структуры файла программы вируса, способов её загрузки и воздействия на EXE-файлы на примере тестовой программы вируса. Его обнаружение и нейтрализация с помощью антивирусного комплекса./ ПО лаборатории Касперского. РЭД ОС LibreOffice.

Тема 5. Файловые вирусы

Ознакомление со способами организации заражения файлов. Изучение структуры файла программы вируса, способов её загрузки и воздействия на COMфайлы на примере тестовой программы вируса. Его обнаружение и нейтрализация с помощью антивирусного комплекса.

Файловые вирусы DOS Классификация по способу использования ресурсов. Классификация по типу заражаемых объектов. Классификация по принципам активации. Классификация по способу организации программного кода. Функционированиея вирусов -«спутников» (вирусы-«компаньоны»). Оверлейные» вирусы. Нерезидентные вирусы. Резидентные вирусы Вирусы -«невидимки».

Технологии заражения «Стандартный» метод заражения. Заражение в середину файла. Заражение в начало файла. Метод предопределенного местоположения файлов. Метод поиска в текущем каталоге. Метод рекурсивного обхода дерева каталогов. Способы выделения вирусом фрагмента памяти. Обработка прерываний. Перехват запуска программы. Перехват файловых операций

Тема 6. Методы защиты от программ деструктивного воздействия

Технологии обнаружения вирусов. Режимы работы антивирусов. Антивирусный комплекс. Комплексная система защиты информации.

«Защита шлюзов»: Общие сведения. Возможные схемы защиты. Требования к антивирусам для шлюзов. Угрозы и методы защиты от них. Эксплуатационные характеристики.

«Защита почтовых систем» Общие сведения. Возможные схемы защиты. Требования к антивирусному комплексу для проверки почтового потока. Unix-системы.

Компьютерные атаки и технологии их обнаружения.

Тема 7. «Защита серверов и рабочих станций

Антивирусный комплекс Kaspersky Administration Kit По Касперского. Ознакомление с процессом инсталляции, принципами работы Kaspersky Administration Kit и способами построения логической сети, задачами удаленной установки и обновления приложений в среде РЕД ОС.

Kaspersky Endpoint Security 11 для Linux Ознакомление с процессом инсталляции, принципами работы Kaspersky Administration Kit и способами построения логической сети, задачами удаленной установки и обновления приложений в среде ОС Linux.

4.3. Содержание практических занятий (очная форма обучения)

Тема 1. Введение в компьютерную вирусологию Появление термина «Компьютерный вирус», военные разработки, возникновение эпидемий компьютерных вирусов. Результат Фреда Коэна. Результат Д. Чесса и С. Вайта. Формализм Ф. Лейтольда. Результат Леонарда Адельмана.
Тема 2. Основные признаки присутствия вредоносных программ и методы по устранению последствий вирусных заражений Использование Диспетчера задач ОС для анализа подозрительных процессов. Анализ

статистку текущих сетевых подключений компьютера с параметрами подключений портов. Установка ClamAV. Настройка обновления. Сканирование системы с помощью ClamAV.Установка ClamTk (графический пользовательский интерфейс для ClamAV) / База знаний РЕД ОС.
Тема 3. Установка Kaspersky для Linux. Изучение руководства по использованию. Инсталяция дистрибутива программы. Установка Агента администрирования.
Тема 4. ЗАРАЖЕНИЕ EXE-файлов Изучение структуры файла программы вируса, способов её загрузки и воздействия на EXE-файлы на примере тестовой программы вируса.
Тема 5. Файловые вирусы Ознакомление со способами организации заражения файлов. Изучение структуры файла программы вируса, способов её загрузки и воздействия на COMфайлы на примере тестовой программы вируса. Его обнаружение и нейтрализация с помощью антивирусного комплекса. Файловые вирусы DOS Классификация по способу использования ресурсов. Классификация по типу заражаемых объектов. Классификация по принципам активации. Классификация по способу организации программного кода.
Тема 6. Методы защиты от программ деструктивного воздействия Технологии обнаружения вирусов. Режимы работы антивирусов. Антивирусный комплекс. Комплексная система защиты информации. «Защита шлюзов»: Общие сведения. Возможные схемы защиты. Требования к антивирусам для шлюзов. Угрозы и методы защиты от них. Эксплуатационные характеристики.
Тема 7. «Защита серверов и рабочих станций Антивирусный комплекс Kaspersky Administration Kit По Касперского. Ознакомление с процессом инсталляции, принципами работы Kaspersky Administration Kit и способами построения логической сети, задачами удаленной установки и обновления приложений в среде РЕД ОС.

4.4. Содержание самостоятельной работы

Тема 1. Введение в компьютерную вирусологию Определение компьютерного вируса. Отличительные особенности компьютерных вирусов и других вредоносных программ. Классификация по способу использования ресурсов. Классификация по типу заражаемых объектов. Классификация по принципам активации. Классификация по способу организации программного кода. Классификация по вредоносным функциям. Классификация по степени опасности
Тема 2. Основные признаки присутствия вредоносных программ и методы по устранению последствий вирусных заражений Загрузка с винчестера. Как устроены загрузочные вирусы. Как загрузочные вирусы получают управление. Как загрузочные вирусы заражают свои жертвы. Как вирусы остаются резидентно в памяти
Тема 3. Установка Kaspersky для Linux. Начальная настройка параметров Агента администрирования. Тестирование программы. / ПО Лаборатории Касперского. РЭД ОС LibreOffice
Тема 4. ЗАРАЖЕНИЕ EXE-файлов Обнаружение и нейтрализация с помощью антивирусного комплекса./ ПО лаборатории Касперского. РЭД ОС LibreOffice.
Тема 5. Файловые вирусы

Функционирование вирусов -«спутников» (вирусы-«компаньоны»). Оверлейные» вирусы. Нерезидентные вирусы. Резидентные вирусы Вирусы -«невидимки». Технологии заражения «Стандартный» метод заражения. Заражение в середину файла. Заражение в начало файла. Метод предопределенного местоположения файлов. Метод поиска в текущем каталоге. Метод рекурсивного обхода дерева каталогов. Способы выделения вирусом фрагмента памяти. Обработка прерываний. Перехват запуска программы. Перехват файловых операций
Тема 6. Методы защиты от программ деструктивного воздействия «Защита почтовых систем» Общие сведения. Возможные схемы защиты. Требования к антивирусному комплексу для проверки почтового потока. Unix-системы. Компьютерные атаки и технологии их обнаружения.
Тема 7. «Защита серверов и рабочих станций Kaspersky Endpoint Security 11 для Linux Ознакомление с процессом инсталляции, принципами работы Kaspersky Administration Kit и способами построения логической сети, задачами удаленной установки и обновления приложений в среде ОС Linux.

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 с оценкой.

Фонд оценочных средств по дисциплине приведен в приложении к РПД.

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

а) основная

1. Бондаренко И.С. Информационная безопасность : учебник / Бондаренко И.С.. — Москва : Издательский Дом МИСиС, 2023. — 254 с. — ISBN 978-5-907560-71-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/137525.html (дата обращения: 10.05.2025). — Режим доступа: для авторизир. пользователей

2. Фомин, Д. В. Информационная безопасность : учебник / Д. В. Фомин. — Москва : Ай Пи Ар Медиа, 2022. — 222 с. — ISBN 978-5-4497-1548-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/118876.html (дата обращения: 03.07.2025). — Режим доступа: для авторизир. пользователей

б) дополнительная

3. Гошко, С. В. Технологии борьбы с компьютерными вирусами : практическое пособие / С. В. Гошко. — Москва : СОЛОН-Пресс, 2021. — 351 с. — ISBN 978-5-91359-059-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/141896.html (дата обращения: 01.08.2025). — 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 проведений 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 достижении 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, «Блокнот», «Microsoft Office Word»);

*программы для демонстрации и создания презентаций (например, «Microsoft PowerPoint»).

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

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