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

Основы информационной безопасности

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 Фурин А.Д. преподаватель

Рабочая программа дисциплины «Основы информационной безопасности» 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.27	**ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**
Цель изучения дисциплины	формирование у студентов знаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты.
Место дисциплины в структуре ОПОП	Дисциплина Основы информационной безопасности относится к базовой части ОПОП и является обязательной для освоения.
Компетенции, формируемые в результате освоения дисциплины	ОПК-4, ОПК-7
Содержание дисциплины	Тема 1. Основные понятия и задачи информационной безопасности. Тема 2 Понятие «угроза безопасности информации». Тема 3 Защита информации. Основные составляющие информационной безопасности – конфиденциальность, целостность, доступность. Тема 4. Взаимодействие процессов. Гонки. Семафоры. Мьютексы Тема 5 Основные составляющие информационной безопасности – конфиденциальность, целостность, доступность. Тема 6. Уязвимости. Методы оценки уязвимости информации
Общая трудоемкость дисциплины	Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 часов)
Форма промежуточной аттестации	Зачет

Содержание

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

Цель изучения дисциплины «Основы информационной безопасности» – формирование у студентов знаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты.

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

Коды компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения по дисциплине
ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1. Знать: основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. ОПК-4.2. Уметь: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. ОПК-4.3. Владеть: составления технической документации на различных этапах жизненного цикла информационной системы
ОПК-7	Способен участвовать в настройке и наладке программно-аппаратных комплексов	ОПК-7.1. Знать: методы настройки, наладки программно-аппаратных комплексов. ОПК-7.2. Уметь: анализировать техническую документацию, производить настройку, наладку и тестирование программно-аппаратных комплексов. ОПК-7.3. Владеть: навыками проверки работоспособности программно-аппаратных комплексов

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина Основы информационной безопасности относится к базовой части ОПОП и является обязательной для освоения, изучается обучающимися очной формы обучения в 5 семестре, очно-заочной формы обучения – в 5 семестре.

Дисциплина является базовой для освоения курсов: «Системное программное обеспечение», «Управление данными» и других дисциплин профессиональной подготовки.

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 3 зачетных единицы (з.е.), 108 академических часа.

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

Для очной формы обучения

Общая трудоёмкость дисциплины составляет 3 зачётных единицы 108 часа

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	108
Контактная работа	38
Аудиторная работа (всего):	38
Лекции	12
Семинары, практические занятия	26
Самостоятельная работа обучающихся (всего)	70
Зачет	+

Для очно-заочной формы обучения

Общая трудоёмкость дисциплины составляет 3 зачётных единицы 108 часа

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	108
Контактная работа	28
Аудиторная работа (всего):	28
Лекции	10
Семинары, практические занятия	18
Самостоятельная работа обучающихся (всего)	80
Зачет	+

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.	. Основные понятия и задачи информационной безопасности.	18	18	2	2	4	2	12	12
2.	Понятие «угроза безопасности информации».	18	18	2	2	4	4	12	12
3.	Понятие «угроза безопасности информации». Классификация Системная классификация угроз безопасности информации.	18	18	2	2	4	4	12	14

	Каналы и методы								
4.	Программные и аппаратные закладки. Примеры. Защита информации. Основные составляющие информационной безопасности – конфиденциальность, целостность, доступность. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации.	18	18	2	1	4	4	12	14
5.	Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Цели и задачи защиты информации. Основные понятия в области защиты информации.	18	18	2	1	4	2	12	14
6.	Уязвимости. Методы оценки уязвимости информации.	18	18	2	2	6	2	10	14
	Всего по дисциплине	**108**	**108**	**12**	**10**	**26**	**18**	**70**	**80**
	Контроль	**-**	**-**						
	Итого	**108**	**108**						

4.2. Содержание дисциплины, структурированное по темам (разделам)

Разделы, темы, дидактические единицы
Лекция 1. Основные понятия и задачи информационной безопасности. Понятие информации и информационной безопасности. Обзор защищаемых объектов и систем. Программное обеспечение для защиты информации
Лекция 2. Понятие «угроза безопасности информации». Понятие «угроза безопасности информации». Доверенная загрузка. Обзор аппаратно-программных устройств защиты информации. Российские компании, работающие в области информационной безопасности. Ресурсы сети Интернет, поисковик уязвимостей.
Лекция 3. Понятие «угроза безопасности информации». Классификация Системная классификация угроз безопасности информации. Каналы и методы несанкционированного доступа к информации. Каналы утечки информации.
Лекция 4. Защита информации. Основные составляющие информационной безопасности – конфиденциальность, целостность, доступность. Программные и аппаратные закладки. Примеры. Защита информации. Основные составляющие информационной безопасности – конфиденциальность, целостность, доступность. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации.

Лекция 5. Основные составляющие информационной безопасности – конфиденциальность, целостность, доступность. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Цели и задачи защиты информации. Основные понятия в области защиты информации.
Лекция 6. Уязвимости. Методы оценки уязвимости информации. Уязвимости. Методы оценки уязвимости информации. Классификации уязвимостей.

4.3. Содержание практических занятий (очная форма обучения)

Разделы, темы, дидактические единицы
1-2. Анализ программных средств защиты информации. Анализ программных средств защиты информации и Российских компаний в области защиты информации
3-4. Анализ методов социальной инженерии и средств борьбы с ней. Анализ методов социальной инженерии и средств борьбы с ней. Исследование источников по социальной инженерии. Подготовка отчёта
5-6. Использование специализированных программных средств для организации защиты информации. Использование специализированных программных средств для организации защиты информации на основе ОС Linux
7-8. Практический анализ уязвимости и работа с калькулятором CVSS Практический анализ уязвимости программных средств, работа с калькулятором CVSS. Составить итоговый отчёт по данной теме согласно стандартным требованиям.
9-10. Практическая работа с техническими средствами по анализу каналов утечки информации Практическая работа с техническими средствами по анализу каналов утечки информации.
11-12. Практическая работа с техническими средствами по формированию, проверке и использованию ЭЦП Практическая работа с техническими средствами по формированию, проверке и использованию ЭЦП
13. Разработка модели угроз безопасности информации согласно заданию Разработка документа – модели угроз безопасности информации согласно заданию.

4.4. Содержание самостоятельной работы

Разделы, темы, дидактические единицы
Тема 1. Основные понятия и задачи информационной безопасности. Обзор защищаемых объектов и систем. Программное обеспечение для защиты информации
Тема 2. Понятие «угроза безопасности информации». Российские компании, работающие в области информационной безопасности. Ресурсы сети Интернет, поисковик уязвимостей.
Тема 3. Понятие «угроза безопасности информации». Классификация Каналы и методы несанкционированного доступа к информации. Каналы утечки информации.

Тема 4. Защита информации. Основные составляющие информационной безопасности – конфиденциальность, целостность, доступность. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации.
Тема 5. Основные составляющие информационной безопасности – конфиденциальность, целостность, доступность. Цели и задачи защиты информации. Основные понятия в области защиты информации.
Тема 6. Уязвимости. Методы оценки уязвимости информации. Классификации уязвимостей.

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. 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: 06.05.2025). — 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 литература:

3. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — 2-е изд. — Саратов : Вузовское образование, 2024. — 214 с. — ISBN 978-5-4487-1026-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/142805.html (дата обращения: 20.03.2025). — 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, «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 учебного кабинета:

- 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.

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