

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

Г.П. Узунова / Г.П. Узунова

«02» февраля 2026 г.

Рабочая программа дисциплины

Основы управления информационной безопасностью

Направление подготовки

10.03.01 «Информационная безопасность»

Профиль

Безопасность компьютерных систем

Квалификация выпускника

Бакалавр

Для всех

форм обучения

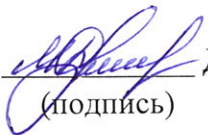
Симферополь, 2026

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 Л. В. Яковенко, старший преподаватель

Рабочая программа дисциплины «Основы управления информационной безопасностью » 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.16	ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
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 зачетные единицы (216 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. 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 «Основы управления информационной безопасностью» – 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 «Основы управления информационной безопасностью» относится к базовой части учебного плана и изучается на 2 курсе в 3 семестре по очной форме обучения.

Для изучения дисциплины студент должен:

- знать основы информационных технологий на предприятии, способы и методы защиты информации;
- уметь пользоваться нормативными документами.

Для успешного освоения дисциплины «Основы управления информационной безопасностью» студент должен изучить курсы

«Программно-аппаратные средства обеспечения информационной безопасности», «Организационное и правовое обеспечение информационной безопасности».

Дисциплина «Основы управления информационной безопасностью» необходима в качестве предшествующей для дисциплин «Информационные технологии и безопасность», «Сети и системы передачи информации» и всех дисциплин, оперирующих информационными технологиями, а также для прохождения научно-исследовательской практики.

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 6 зачетных единицы (з.е.), 216 академических часа.

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

Для очной формы обучения

Общая трудоемкость дисциплины составляет 6 зачётных единицы 216 часа

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	216
Контактная работа	54
Аудиторная работа (всего):	54
Лекции	36
Семинары, практические занятия	18
Самостоятельная работа обучающихся (всего)	126
Курсовая работа	
Экзамен	36

Для очно-заочной формы обучения

Общая трудоемкость дисциплины составляет 6 зачётных единицы 216 часа

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	216
Контактная работа	48
Аудиторная работа (всего):	48
Лекции	14
Семинары, практические занятия	34
Самостоятельная работа обучающихся (всего)	132
Контрольная работа	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 трудоемкость 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.	Введение	12	12	2	1	2	2	9	9
2.	Задачи и принципы организации службы информационной безопасности			2	1	2	2	9	9

3.	Создание службы информационной безопасности. Требования к сотрудникам СИБ.	12	12	2	1	2	2	9	9
4	Инвентаризация информационных систем Классификация информационных систем	12	12	1	1	2	2	9	9
5	Классификация объектов и субъектов информационных отношений	12	12	1	1	2	2	9	9
6	Оценка информационных рисков. Управление информационными рисками.	12	12	1	1	4	4	9	9
7	Работа службы информационной безопасности с оборудованием информационных систем.	12	12	1	1	4	4	9	9
8	Работа службы Информационной безопасности с персоналом	12	12	1	1	4	4	9	9
9	Создание политики информационной безопасности.	14	14	1	1	4	2	9	9
10	Создание механизмов информационной безопасности и их тестирование	14	14	1	1	4	2	9	10
11	Создание аварийного плана. Состав и содержание документов.	14	14	1	1	2	2	9	10
12	Работа службы Информационной безопасности с аварийным планом.	14	14	1	1	2	2	9	10
13	Работа службы информационной безопасности при нарушении правил защиты информации	14	14	1	1	2	2	9	10
14	Расследование и анализ нарушений в сфере информационной безопасности.	14	14	2	1	2	2	9	10
	Контроль	36	36						
	Итого	216	216	18	14	38	34	126	132

4.2. Содержание дисциплины, структурированное по темам (разделам)

Введение

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

Тема 1. Задачи и принципы организации службы информационной безопасности

Задачи службы информационной безопасности (СИБ). Варианты организации работы СИБ. Оценка эффективности работы СИБ. Контроль за работой СИБ

Тема 2. Создание службы информационной безопасности. Требования к сотрудникам СИБ

Критерии необходимости создания СИБ. Функции СИБ. Типовая структура СИБ. Требования стандарта SSCP к специалистам по защите информации. Методика подбора кадров СИБ.

Тема 3. Инвентаризация информационных систем Классификация информационных систем

Общий характер инвентаризации информационных систем. Принципы и направления инвентаризации. Объем собираемой информации. Контроль инвентаризации. Терминология и постановка задачи классификации. Основные регламенты классификации. Оранжевая и Красная книги. Контроль классификации.

Тема 4. Классификация объектов и субъектов информационных отношений

Типовые сферы применения классификации объектов. Модель классификации по наличию, по модификации, по конфиденциальности. Требования к функциональной безопасности. Требования к достоверности безопасности. Субъекты информационного пространства. Принципы распределения прав и ответственности субъектов. Модель классификации информационных субъектов. Сопоставление ролей функциональным обязанностям. Сопоставление ролей классам обрабатываемой информации.

Тема 5 Оценка информационных рисков. Управление информационными рисками.

Модель качественной оценки информационных рисков. Модель обобщенного стоимостного результата. Количественная модель оценки информационных рисков.

Определение вероятности информационного события. Определение стоимости информационных активов. Построение модели нарушителя. Рейтинги информационных атак. Современные методы анализа и контроля рисков информационных систем.

Тема 6 Работа службы информационной безопасности с оборудованием информационных систем.

Области безопасности корпорации. Методика работы СИБ с оборудованием. Проверка оборудования. Обеспечение сохранности оборудования. Защита от ПЭМИН.

Тема 7 Работа службы Информационной безопасности с персоналом.

Общие вопросы работы СИБ с персоналом. Контроль приема на работу. Проверка квалификации сотрудников как субъектов информационных отношений. Методическая работа с персоналом. Работа с бывшими кадрами.

Тема 8 Создание политики информационной безопасности.

Документы политики информационной безопасности. Концепция информационной безопасности. Стандарты информационной безопасности. Процедуры информационной безопасности. Методы информационной безопасности.

Тема 9 Создание механизмов информационной безопасности и их тестирование

Общие вопросы тестирования процедур и механизмов безопасности. Классификация тестов. Дружеский взлом. Обратная связь от пользователей. Порядок и методика тестирования. Анализ результатов тестирования.

Тема 10 Создание аварийного плана. Состав и содержание документов.

Понятие аварийного плана. Принципы создания аварийного плана. Состав и содержание документов плана. Классификация возможных событий. Классификация объектов по приоритетам. Создание шкалы резервных объектов. Определение аварийных ситуаций.

Тема 11 Работа службы Информационной безопасности с аварийным планом.

Тестирование аварийного плана. Предварительные мероприятия плана. Мероприятия, проводимые СИБ во время аварии. Методика сокращения предполагаемого

ущерба. Сохранение данных во время аварии. Возвращение к нормальной работе (в штатный режим). Анализ аварийных ситуаций.

Тема 12 Работа службы информационной безопасности при нарушении правил защиты информации.

Понятие группы реагирования. Основы функционирования группы реагирования. Минимальный контроль безопасности. Обязательная периодичность работ. Контроль событий безопасности. Постоянные работы и мониторинг.

Тема 13 Расследование и анализ нарушений в сфере информационной безопасности.

Нормативная база для проведения расследований. Определение целей и задач расследования. Наблюдение за нарушителем. Сбор улик.

4.3. Содержание практических занятий (очная форма обучения)

Практическое занятие 1. Разработка политики информационной безопасности для условной компании (определение целей, области применения, ролей и ответственности).

Практическое занятие 2. Проведение анализа информационных активов организации и составление их реестра с присвоением уровней критичности.

Практическое занятие 3. Идентификация актуальных угроз информационной безопасности на основе банка данных ФСТЭК России (*БДУ*) применительно к веб-серверу предприятия.

Практическое занятие 4 Оценка рисков ИБ методом *CRAMM* или матрицей вероятности и ущерба для бизнес-процесса «Прием платежей».

Практическое занятие 5. Разработка плана обработки рисков: выбор стратегии (снижение, принятие, уклонение, передача) и обоснование контрмер для выявленных уязвимостей.

Практическое занятие 6. Проектирование системы управления информационной безопасностью (СУИБ) в соответствии с требованиями стандарта ISO/IEC 27001: построение контекстной диаграммы процессов.

Практическое занятие 7. Разработка матрицы доступа (*MAC*) и модели ролевого разграничения прав (*RBAC*) для сотрудников бухгалтерии.

Практическое занятие 8. Составление регламента резервного копирования и восстановления информации после сбоя (включая расчет целевого времени восстановления — *RTO*, и целевой точки восстановления — *RPO*).

Практическое занятие 9. Разработка положения об обучении персонала основам кибергигиены и проведение теста на фишинговую грамотность (моделирование атаки).

Практическое занятие 10 Формирование алгоритма реагирования на инцидент ИБ типа «заражение корпоративной сети шифровальщиком» согласно стандарту NIST SP 800-61.

Практическое занятие 11 Расчет показателей эффективности (*KPI*) службы информационной безопасности и заполнение дашборда мониторинга состояния СУИБ.

Практическое занятие 12 Аудит соответствия требованиям законодательства РФ по защите персональных данных (152-ФЗ): проверка наличия необходимых согласий и локальных актов.

Практическое занятие 13 Разработка технического задания на внедрение средства защиты информации (например, межсетевого экрана нового поколения или *DLP*-системы).

Практическое занятие 14 Подготовка отчета об аудите информационной безопасности: описание выявленных несоответствий, оценка уровня зрелости процессов и выдача рекомендаций.

4.4. Содержание самостоятельной работы

№ п/п	Вид самостоятельной работы	Наименование работы и содержание
1	Контрольная работа	Определение процедур информационной безопасности предприятия
2	Самостоятельное изучение онлайн-курса	Онлайн-курс «Основы управления информационной безопасностью» https://farvater.gumrf.ru/course/view.php?

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 – экзамен. Форма проведения промежуточной аттестации – письменный экзамен.

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. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 5-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2026. — 266 с. — ISBN 978-5-4497-3316-0. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/162521/details> (дата обращения: 27.01.2026). — Режим доступа: для авторизир. пользователей

2. Мартынов, А. П. Информационная безопасность и защита информации : учебное пособие / А. П. Мартынов, И. А. Мартынова, А. А. Русаков. — 2-е изд. — Москва : Ай Пи Ар Медиа, 2026. — 130 с. — ISBN 978-5-4497-2349-9. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/155918/details> (дата обращения: 27.01.2026). — Режим доступа: для авторизир. пользователей.

3. Белаш, В. Ю. Информационно-коммуникационные технологии : учебно-методическое пособие / В. Ю. Белаш, А. А. Салдаева. — Москва : Ай Пи Ар Медиа, 2021. — 72 с. — ISBN 978-5-4497-1390-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/111181.html> (дата обращения: 16.01.2026). — Режим доступа: для авторизир. пользователей.

б) дополнительная литература:

4. Основы информационных технологий : учебное пособие / С. В. Назаров, С. Н. Белоусова, И. А. Бессонова [и др.]. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 530 с. — ISBN 978-

5-4497-0339-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/89454.html> (дата обращения: 16.01.2026). — 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.