

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:

fd935d10451b860e912264c037858448452b603f94388008e29877a6bcbf5

**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

**Организационное и правовое обеспечение информационной
безопасности**

Направление подготовки

10.03.01 «Информационная безопасность»

Профиль

Безопасность компьютерных систем

Квалификация выпускника

Бакалавр

Для всех

форм обучения

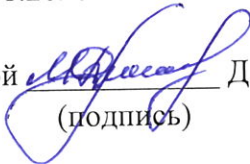
Симферополь, 2026

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 «Организационное и правовое обеспечение информационной безопасности» утверждена на заседании кафедры «Управление и бизнес-информатика».

Протокол № 6 от 29.01.2026 г.

Заведующий кафедрой  Д.В. Моторина
(подпись)

Индекс дисциплины по учебному плану	Наименование дисциплины
Б1.О.17	ТЕОРИЯ ВЕРОЯТНОСТЕЙ И МАТЕМАТИЧЕСКАЯ СТАТИСТИКА
Цель изучения дисциплины	Формирование компетенций, направленных на развитие научного мировоззрения, представления о современной картине мира, приобретение фундаментальных знаний и овладение основными приемами и методами познавательной деятельности как основой будущей профессиональной деятельности.
Место дисциплины в структуре ОПОП	Дисциплина относится к обязательной части блока 1. «Дисциплины (модули)» программы бакалавриата
Компетенции, формируемые в результате освоения дисциплины	ОПК-4, ОПК-11
Содержание дисциплины	Тема 1. Правовые основы информационной безопасности. Тема 2. Правовые режимы информации ограниченного доступа. Тема 3. Персональные данные и обязанности оператора. Тема 4. Политика и локальные документы. Тема 5. Активы, риски и организационные меры. Тема 6. Управление доступом и персоналом. Тема 7. Договорная работа и взаимодействие и третьими лицами. Тема 8. Инциденты и внутренний контроль. Тема 9. Ответственность и актуализация системы защиты.
Общая трудоемкость дисциплины	Общая трудоемкость дисциплины составляет 36 зачетных 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	6
6. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	10
7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	11
8. Методические указания для обучающихся по освоению дисциплины	12
9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)	12
10. Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине	12
Приложение к РПД	13

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

Целью изучения дисциплины «Организация и правовое обеспечение информационной безопасности» является формирование у обучающихся системы фундаментальных знаний о физических законах и явлениях природы, развитие научного мировоззрения и физического мышления, а также овладение методами научного познания и практическими навыками применения физических законов при решении профессиональных и прикладных задач.

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 применять необходимые физические законы и модели для решения задач профессиональной деятельности	ОПК-4.1. Применяет физические явления и эффекты для решения практических задач ОПК-4.2. Анализирует процессы, протекающие в линейных и нелинейных электрических цепях, с применением методов анализа в переходных и установившихся режимах в частотной и временной областях ОПК-4.3. Использует принципы работы элементов и функциональных узлов электронной аппаратуры при исследовании средств защиты информации
ОПК-11	Способен проводить эксперименты по заданной методике и обработку их результатов	ОПК-11.1. Проводит физический эксперимент, обрабатывает его результаты ОПК-11.2. Использует стандартные вероятностно-статистические методы анализа экспериментальных данных

2. Место дисциплины в структуре ОПОП ВО

Дисциплина Б1.О.17 «Организация и правовое обеспечение информационной безопасности» относится к обязательной части блока 1. «Дисциплины (модули)» учебного плана ОПОП бакалавриата по направлению подготовки 10.03.02 «Информационная безопасность».

Дисциплина «Теория вероятностей и математическая статистика» изучается обучающимися очной формы обучения в 5-6 семестре, очно-заочной формы обучения – в 5-6 семестре.

При изучении данной дисциплины обучающийся использует знания, умения и навыки, которые сформированы в процессе изучения предшествующих дисциплин: «высшая математика», «информационные технологии в профессиональной деятельности».

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 36 зачетных единиц (з. е.), 216 академических часа.

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

Для очной формы обучения

Общая трудоёмкость дисциплины составляет 8 зачётных единицы 288 часа

Объём дисциплины	Всего часов
Общая трудоёмкость дисциплины	216
Контактная работа	96
Аудиторная работа (всего):	96
Лекции	32
Семинары, практические занятия	64
Самостоятельная работа обучающихся (всего)	84
Экзамен	36

Для очно-заочной формы обучения

Общая трудоёмкость дисциплины составляет 8 зачётных единицы 288 часа

Объём дисциплины	Всего часов
Общая трудоёмкость дисциплины	216
Контактная работа	40
Аудиторная работа (всего):	40
Лекции	16
Семинары, практические занятия	24
Самостоятельная работа обучающихся (всего)	140
Зачет	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.	Правовые основы информационной безопасности.	20	20	4	2	8	4	8	8
2.	Правовые режимы информации ограниченного доступа.	20	20	4	2	8	4	8	8
3.	Персональные данные и обязанности оператора.	20	20	4	2	8	4	8	8
4.	Политика и локальные документы.	20	20	4	2	8	2	8	8
5.	Активы, риски и организационные меры.	20	20	4		8	2	8	8
6.	Управление доступом и	20	20	4	2	8	2	8	8

	персоналом.								
7.	Договорная работа и взаимодействие с третьими лицами.	20	20	4	2	8	2	8	8
8.	Инциденты и внутренний контроль.	20	20	2	2	4	2	8	8
9.	Ответственности и актуализация системы защиты.	20	20	2	0	4	2	8	8
Всего по дисциплине		180	180	32	16	64	24	72	72
Экзамен		36	36						
Итого		216	216						

4.2 Содержание дисциплины (модуля), структурированное по разделам (темам)

Тема 1. Правовые основы информационной безопасности.

Система источников права и сфера действия нормативных актов. Информация, обладатель информации, доступ и ограничение доступа. Соотношение закона, подзаконного и локального акта.

Тема 2. Правовые режимы информации ограниченного доступа.

Конфиденциальная информация, коммерческая тайна, профессиональные и служебные ограничения. Особенности правового режима и его установления. Документирование перечней и условий допуска.

Тема 3. Персональные данные и обязанности оператора.

Цели и основания обработки, минимизация данных, права субъектов, сроки хранения, внутренний учет процессов и защита данных.

Тема 4. Политика и локальные документы.

Структура политики информационной безопасности, положения о доступе и обращении с носителями, инструкции работников. Порядок согласования, доведения и пересмотра документов.

Тема 5. Активы, риски и организационные меры.

Реестр политики информационной безопасности, положения о доступе и обращении с носителями, инструкции работников. Порядок согласования, доведения и пересмотра документов.

Тема 6. Управление доступом и персоналом.

Ролевой доступ и минимально необходимые полномочия. Жизненный цикл учетной записи. Обучение, кадровые изменения, допуск подрядчиков и учет носителей.

Тема 7. Договорная работа и взаимодействие с третьими лицами.

Требования к защите информации в договоре, распределение обязанностей сторон, порядок передачи, возврата и удаления сведений. Документирование контроля исполнения.

Тема 8. Инциденты и внутренний контроль.

Регистрация событий и инцидентов, первичные действия, установление обстоятельств, сохранение материалов, корректирующие меры. План внутренней проверки.

Тема 9. Ответственность и актуализация системы защиты.

Виды юридической и дисциплинарной ответственности в зависимости от обстоятельств нарушения. Поддержание локальных документов и организационных мер в актуальном состоянии.

4.3. Темы практических занятий

Тема 1. Правовые основы информационной безопасности.

1. Составление карты источников для условной организации.
2. Проверка актуальной редакции области применения нормы.

Тема 2. Правовые режимы информации ограниченного доступа.

1. Сравнение правовых режимов.
2. Проект перечня защищаемых сведений и порядка маркирования носителей.
- 3.

Тема 3. Персональные данные и обязанности оператора.

1. Матрица «цель – данные – операция – ответственность».
2. Маршрут рассмотрения запроса субъекта данных.

Тема 4. Политика и локальные документы.

1. Разработка оглавления политики и фрагмента инструкции.
2. Оценка исполнимости процедур.

Тема 5. Активы, риски и организационные меры.

1. Формирование реестра активов и рисков.
2. Приоритизация мер по условному сценарию.

Тема 6. Управление доступом и персоналом.

1. Матрица ролей и прав.
2. Регламент заявки, согласования и отзыва временного доступа.

Тема 7. Договорная работа и взаимодействие с третьими лицами.

1. Проект раздела договора с подрядчиком.

2. Чек-лист допуска внешнего специалиста.
Тема 8. Инциденты и внутренний контроль.
1. Карточка инцидента, план проверки доступа, акт несоответствия и график устранения.
Тема 9. Ответственность и актуализация системы защиты.
1. Комплексный кейс: план защиты условной организации, матрица ответственности, программа внутреннего контроля.

4.4. Содержание самостоятельной работы

Тема 1. Правовые основы информационной безопасности.
3. Составление карты источников для условной организации. 4. Проверка актуальной редакции области применения нормы.
Тема 2. Правовые режимы информации ограниченного доступа.
4. Сравнение правовых режимов. 5. Проект перечня защищаемых сведений и порядка маркирования носителей. 6.
Тема 3. Персональные данные и обязанности оператора.
3. Матрица «цель – данные – операция – ответственность». 4. Маршрут рассмотрения запроса субъекта данных.
Тема 4. Политика и локальные документы.
3. Разработка оглавления политики и фрагмента инструкции. 4. Оценка исполнимости процедур.
Тема 5. Активы, риски и организационные меры.
3. Формирование реестра активов и рисков. 4. Приоритизация мер по условному сценарию.
Тема 6. Управление доступом и персоналом.
3. Матрица ролей и прав.

4. Регламент заявки, согласования и отзыва временного доступа.
Тема 7. Договорная работа и взаимодействие с третьими лицами. 3. Проект раздела договора с подрядчиком. 4. Чек-лист допуска внешнего специалиста.
Тема 8. Инциденты и внутренний контроль. 2. Карточка инцидента, план проверки доступа, акт несоответствия и график устранения.
Тема 9. Ответственность и актуализация системы защиты. 2. Комплексный кейс: план защиты условной организации, матрица ответственности, программа внутреннего контроля.

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 в целом по дисциплине – письменный зачет.

Оценочные средства по дисциплине приведены в Приложении к РПД.

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

а) основная литература:

1. Хорев, П. Б. Программно-аппаратная защита информации : учебник и практикум для вузов / П. Б. Хорев. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 367 с. — ISBN 978-5-534-16542-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/535678> (дата обращения: 29.09.2026). — Режим доступа: для авторизир. пользователей.

2. Галицкий, А. В. Технологии безопасности информационно-вычислительных систем и сетей : учебное пособие / А. В. Галицкий, С. Д. Рябко, В. Ф. Шаньгин. — Москва : Солон-Пресс, 2023. — 704 с. — ISBN 978-5-91359-524-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/130583.html> (дата обращения: 29.09.2026). — Режим доступа: для авторизир. пользователей.

3. Гришина, Н. В. Организация комплексной системы защиты информации : учебное пособие / Н. В. Гришина. — Москва : ФОРУМ : ИНФРА-М, 2022. — 256 с. — ISBN 978-5-00091-722-0. — Текст : электронный // Znanium.com : [сайт]. — URL: <https://znanium.com/catalog/product/1865456> (дата обращения: 29.09.2026). — Режим доступа: для авторизир. пользователей.

4. Мельников, В. П. Информационная безопасность и защита информации : учебник / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под редакцией С. А. Клейменова. — 8-е изд., стер. — Москва : Академия, 2023. — 336 с. — ISBN 978-5-4468-9876-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/140566.html> (дата обращения: 29.09.2026). — Режим доступа: для авторизир. пользователей.

5. Парошин, А. А. Нормативно-правовые основы защиты информации : учебное пособие / А. А. Парошин. — Владивосток : Дальневосточный федеральный университет, 2024. — 112 с. — ISBN 978-5-7444-5589-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/128415.html> (дата обращения: 29.09.2026). — Режим доступа: для авторизир. пользователей.

б) дополнительная литература:

6. Лукацкий, А. В. Обнаружение атак / А. В. Лукацкий. — 2-е изд. — Москва : ДМК Пресс, 2023. — 598 с. — ISBN 978-5-97060-987-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/146776.html> (дата обращения: 29.09.2026). — Режим доступа: для авторизир. пользователей.

7. Едомский, Д. Защита информации при реализации государственных информационных проектов / Д. Едомский // Администратор информационных технологий. — 2023. — № 9. — С. 76–78. — Текст : электронный. — URL: <https://www.meteorf.gov.ru/documents/21/10770/.^2>

8. Черкас, Ю. Защита от современных кибератак: мифы и реальность / Ю. Черкас // Администратор информационных технологий. — 2023. — № 9. — С. 40–43. — Текст : электронный. — URL: <https://www.meteorf.gov.ru/documents/21/10770/.^2>

9. Громов, И. Безопасность информации на государственном уровне / И. Громов // Администратор информационных технологий. — 2023. — № 9. — С. 20–24. — Текст : электронный. — URL: <https://www.meteorf.gov.ru/documents/21/10770/.^2>

10. Старостина, Е. Мишень социальной инженерии — это вы сами / Е. Старостина, Е. Хрусталева // Администратор информационных технологий. — 2023. — № 9. — С. 64–67. — Текст : электронный. — URL: <https://www.meteorf.gov.ru/documents/21/10770/.^2>

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

1. ФСТЭК России (Федеральная служба по техническому и экспортному контролю) : официальный сайт. — URL: <https://fstec.ru> — Текст : электронный.

2. ФСБ России (Центр защиты информации и специальной связи) : официальный сайт. — URL: <https://fsb.ru/fsb/supplement.htm> — Текст : электронный.

3. Министерство цифрового развития, связи и массовых коммуникаций РФ : официальный сайт. — URL: <https://digital.gov.ru> — Текст : электронный.

4. Реестр российского программного обеспечения : официальный сайт. — URL: <https://reestr.digital.gov.ru> — Текст : электронный.

5. Портал «Госуслуги» (раздел «Безопасность в сети») : официальный сайт. — URL: <https://www.gosuslugi.ru> — Текст : электронный.

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

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

8. Научная электронная библиотека «КиберЛенинка» : официальный сайт. — URL: <https://cyberleninka.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, «Google chrome»);
- *программы, демонстрации видео материалов (например, проигрыватель «Windows Media Player»);
- *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 ;
- комплект учебно-наглядных пособий;
- комплект электронных видеоматериалов.

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