

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:

fd935d10451b860e912264c0378f8448452bfdb603f94388008e29877a6bcbf5

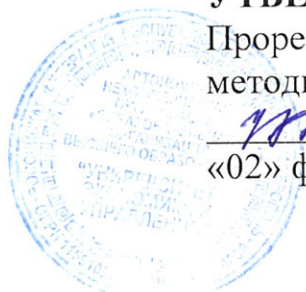
**АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
«ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ»
«УНИВЕРСИТЕТ ЭКОНОМИКИ И УПРАВЛЕНИЯ»
Факультет экономики, управления и юриспруденции**

Кафедра «Управление и бизнес-информатика»

УТВЕРЖДАЮ

Проректор по учебно-методической работе

 / Г.П. Узунова
«02» февраля 2026 г.



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Правовое обеспечение защиты информации

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 Яковенко Л.В., преподаватель

Рабочая программа дисциплины «Правовое обеспечение защиты информации» 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.02.01	Правовое обеспечение защиты информации
Цель изучения дисциплины	формирование у студентов системного понимания нормативно-правовой базы Российской Федерации в области обеспечения информационной безопасности. Дисциплина направлена на изучение прав, обязанностей и ответственности граждан, организаций и государства при работе с информацией ограниченного доступа
Место дисциплины в структуре ОПОП	Дисциплина относится к части, формируемой участниками образовательных отношений блока 1 программы бакалавриата.
Компетенции, формируемые в результате освоения дисциплины	ПК-5
Содержание дисциплины	Тема 1. Конституционные основы информационного права и государственная политика РФ в сфере ИБ. Тема 2. Федеральное законодательство об информации: ФЗ №149-ФЗ и классификация сведений Тема 3. Защита персональных данных: ФЗ №152-ФЗ и работа с субъектами ПДн. Тема 4. Правовая защита государственной тайны: Закон РФ №5485-1 и система лицензирования. Тема 5. Коммерческая тайна и интеллектуальная собственность в ИТ-сфере. Тема 6. Уголовная, административная и гражданская ответственность в сфере компьютерной информации. Тема 7. Регулирование использования криптографических средств и трансграничной передачи данных.
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	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	6
4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий	7
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	12
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	13

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

Цель изучения дисциплины «Правовое обеспечение защиты информации» – формирование у студентов системного понимания нормативно-правовой базы Российской Федерации в области обеспечения информационной безопасности. Дисциплина направлена на изучение прав, обязанностей и ответственности граждан, организаций и государства при работе с информацией ограниченного доступа.

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-5	Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	ПК-5.1. Знает принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации); ПК-5.2. владеет методами организации и управления деятельностью служб защиты информации на предприятии

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина Б1.В.ДВ.02.01 «Правовое обеспечение защиты информации» относится к части, формируемой участниками образовательных отношений блока 1 учебного плана ОПОП бакалавриата по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина «Правовое обеспечение защиты информации» изучается обучающимися очной формы обучения во 4 семестре, очно-заочной формы обучения – во 4 семестре.

При изучении данной дисциплины обучающийся использует знания, умения и навыки, которые сформированы в процессе изучения предшествующих дисциплин: «Теория алгоритмов», «Теория информационных процессов и систем» 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 трудоёмкость 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 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. Конституционные основы информационного права и государственная политика РФ в сфере ИБ.	18	18	2	2	2	2	14	14
2.	Тема 2. Федеральное законодательство об информации: ФЗ №149-ФЗ и классификация сведений	18	18	4	2	2	2	12	14
3.	Тема 3. Защита персональных данных: ФЗ №152-ФЗ и работа с субъектами ПДн.	18	18	4	2	4	2	10	14
4.	Тема 4. Правовая защита государственной тайны: Закон РФ №5485-1 и система лицензирования.	18	18	4	2	4	2	10	14

5.	Тема 5. Коммерческая тайна и интеллектуальная собственность в ИТ-сфере.	18	18	4	4	4	4	10	10
6.	Тема 6. Уголовная, административная и гражданская ответственность в сфере компьютерной информации.	36	36	2	2	4	4	30	30
7.	Тема 7. Регулирование использования криптографических средств и трансграничной передачи данных.	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. Конституционные основы информационного права и государственная политика РФ в сфере ИБ Раскрывается право граждан на поиск, получение и передачу информации (ст. 29 Конституции РФ), а также право на неприкосновенность частной жизни и личную тайну (ст. 23, 24). Изучается Доктрина информационной безопасности РФ как документ стратегического планирования, определяющий национальные интересы и угрозы в информационном пространстве.

Тема 2. Федеральное законодательство об информации: ФЗ №149-ФЗ и классификация сведений Детально рассматривается базовый закон «Об информации, информационных технологиях и о защите информации». Изучаются категории информации по уровню доступа: общедоступная информация и информация ограниченного доступа (государственная тайна, коммерческая тайна, служебная тайна, персональные данные). Разбирается правовой статус обладателя информации и оператора информационной системы.

Тема 3. Защита персональных данных: ФЗ №152-ФЗ и работа с субъектами ПДн Изучаются правовые механизмы обработки личной информации граждан. Рассматриваются обязанности операторов (уведомление Роскомнадзора, назначение ответственного за организацию обработки ПДн), требования к локализации баз данных на территории РФ и порядок получения согласия субъекта. Анализируется деятельность регулятора — Роскомнадзора.

Тема 4. Правовая защита государственной тайны: Закон РФ №5485-1 и система лицензирования Раскрывается иерархия секретности («особой важности», «совершенно секретно», «секретно»). Изучается процедура оформления допуска должностных лиц и сотрудников предприятий к гостайне. Особое внимание уделяется системе лицензирования деятельности в области защиты гостайны (ФСБ России) и технической защиты конфиденциальной информации (ФСТЭК России).

Тема 5. Коммерческая тайна и интеллектуальная собственность в ИТ-сфере Рассматривается режим охраны ноу-хау согласно ФЗ №98 «О коммерческой тайне». Изучаются способы передачи исключительных прав на программное обеспечение и базы данных (договоры авторского заказа, лицензионные соглашения). Анализируется ответственность за промышленный шпионаж и нарушение патентных прав.

Тема 6. Уголовная, административная и гражданская ответственность в сфере компьютерной информации Анализируются составы преступлений из главы 28 УК РФ: неправомерный доступ к компьютерной информации (ст. 272), создание и использование вредоносных программ (ст. 273), нарушение правил эксплуатации СИИ (ст. 274). Рассматриваются статьи КоАП РФ за нарушение правил защиты информации и порядок возмещения материального ущерба в рамках гражданского судопроизводства.

Тема 7. Регулирование использования криптографических средств и трансграничной передачи данных Изучаются правила ввоза, вывоза и эксплуатации средств криптографической защиты информации (СКЗИ). Раскрываются полномочия ФСБ России в области регулирования шифрования. Рассматривается правовой механизм уведомления государственных органов о намерении осуществлять трансграничную передачу персональных данных и основания для запрета такой передачи.

4.3. Содержание практических занятий (очная форма обучения)

Разделы, темы, содержание
Тема 1. Конституционные основы информационного права и государственная политика РФ в сфере ИБ Раскрывается право граждан на поиск, получение и передачу информации (ст. 29 Конституции РФ), а также право на неприкосновенность частной жизни и личную тайну (ст. 23, 24).
Тема 2. Федеральное законодательство об информации: ФЗ №149-ФЗ и классификация сведений Детально рассматривается базовый закон «Об информации, информационных технологиях и о защите информации». Изучаются категории информации по уровню доступа: общедоступная информация и информация ограниченного доступа (государственная тайна, коммерческая тайна, служебная тайна, персональные данные).
Тема 3. Защита персональных данных: ФЗ №152-ФЗ и работа с субъектами ПДн Изучаются правовые механизмы обработки личной информации граждан. Рассматриваются обязанности операторов (уведомление Роскомнадзора, назначение ответственного за организацию обработки ПДн), требования к локализации баз данных на территории РФ и порядок получения согласия субъекта.
Тема 4. Правовая защита государственной тайны: Закон РФ №5485-1 и система лицензирования Раскрывается иерархия секретности («особой важности», «совершенно секретно», «секретно»). Изучается процедура оформления допуска должностных лиц и сотрудников предприятий к гостайне.
Тема 5. Коммерческая тайна и интеллектуальная собственность в ИТ-сфере Рассматривается режим охраны ноу-хау согласно ФЗ №98 «О коммерческой тайне». Изучаются способы передачи исключительных прав на программное обеспечение и базы данных (договоры авторского заказа, лицензионные соглашения).
Тема 6. Уголовная, административная и гражданская ответственность в сфере компьютерной информации Анализируются составы преступлений из главы 28 УК РФ: неправомерный доступ к компьютерной информации (ст. 272), создание и использование вредоносных программ (ст. 273), нарушение правил эксплуатации СИИ (ст. 274).
Тема 7. Регулирование использования криптографических средств и трансграничной передачи данных Изучаются правила ввоза, вывоза и эксплуатации средств криптографической защиты информации (СКЗИ). Раскрываются полномочия ФСБ России в области регулирования шифрования.

4.4. Содержание самостоятельной работы

Разделы, темы, содержание
Тема 1. Конституционные основы информационного права и государственная политика РФ в сфере ИБ Доктрина информационной безопасности РФ как документ стратегического планирования, определяющий национальные интересы и угрозы в информационном пространстве.
Тема 2. Федеральное законодательство об информации: ФЗ №149-ФЗ и классификация сведений Разбирается правовой статус обладателя информации и оператора информационной системы.
Тема 3. Защита персональных данных: ФЗ №152-ФЗ и работа с субъектами ПДн Анализируется деятельность регулятора — Роскомнадзора.
Тема 4. Правовая защита государственной тайны: Закон РФ №5485-1 и система лицензирования Система лицензирования деятельности в области защиты гостайны (ФСБ России) и технической защиты конфиденциальной информации (ФСТЭК России).
Тема 5. Коммерческая тайна и интеллектуальная собственность в ИТ-сфере Анализируется ответственность за промышленный шпионаж и нарушение патентных прав.
Тема 6. Уголовная, административная и гражданская ответственность в сфере компьютерной информации Рассматриваются статьи КоАП РФ за нарушение правил защиты информации и порядок возмещения материального ущерба в рамках гражданского судопроизводства.
Тема 7. Регулирование использования криптографических средств и трансграничной передачи Правовой механизм уведомления государственных органов о намерении осуществлять трансграничную передачу персональных данных и основания для запрета такой передачи.

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. Организация защиты информации объекта информатизации : учебное пособие / К. А. Седаков, М. Л. Гулак, С. В. Даньков [и др.]. — Москва : Ай Пи Ар Медиа, 2026. — 302 с. — ISBN 978-5-4497-5648-0. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/162326/details> (дата обращения: 27.01.2026). — DOI: <https://doi.org/10.23682/162326>. — Режим доступа: для авторизир. пользователей
2. Кухаренко, Т. А. Правовое обеспечение профессиональной деятельности ИТ-специалистов : учебник для СПО / Т. А. Кухаренко, Г. А. Хачатрян, И. В. Кузнецова. — 2-е изд. — Саратов : Профобразование, 2024. — 303 с. — ISBN 978-5-4488-1999-5. — Текст

: электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/138460/details> (дата обращения: 27.09.2026). — Режим доступа: для авторизир. пользователей

б) дополнительная

3. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. — 3-е изд. — Саратов : Профобразование, 2024. — 543 с. — ISBN 978-5-4488-0074-0. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/145909/details> (дата обращения: 27.01.2026). — 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, «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 учебного кабинета:

- 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.