

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:

fd935d10451b860e912264c03783448457bf607f94388008e39877a6bcb6f

**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

**Комплексное обеспечение защиты информации объекта
информатизации**

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 Фурин А.Д., преподаватель

Рабочая программа дисциплины «Комплексное обеспечение защиты информации объекта информатизации» 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.32	Комплексное обеспечение защиты информации объекта информатизации
Цель изучения дисциплины	формирование у студентов профессиональных компетенций, необходимых для проектирования, создания и управления комплексной системой защиты информации (КСЗИ) как единого организационно-технического механизма
Место дисциплины в структуре ОПОП	Дисциплина Комплексное обеспечение защиты информации относится к базовой части ОПОП и является обязательной для освоения.
Компетенции, формируемые в результате освоения дисциплины	ОПК-10
Содержание дисциплины	Тема 1. Системный анализ объекта информатизации и классификация информационных активов. Тема 2. Моделирование угроз безопасности информации и формирование модели нарушителя. Тема 3. Разработка комплексной системы защиты информации (КСЗИ): организационные и инженерно-технические меры. Тема 4. Обеспечение защиты информации при использовании технологий виртуализации и облачных вычислений Тема 5. Оценка эффективности системы защиты и экономический анализ затрат на информационную безопасность. Тема 6. Аттестация объектов информатизации и сопровождение жизненного цикла КСЗИ.
Общая трудоемкость дисциплины	Общая трудоемкость дисциплины составляет 4 зачетных единиц (144 часов)
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	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. 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	13
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	14

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

Цель изучения дисциплины – формирование у студентов профессиональных компетенций, необходимых для проектирования, создания и управления комплексной системой защиты информации (КСЗИ) как единого организационно-технического механизма.

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-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 соответствующих проектных решений	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 «Комплексное обеспечение защиты информации объекта информатизации» относится к базовой части ОПОП и является обязательной для освоения, изучается обучающимися очной формы обучения в 7 семестре, очно-заочной формы обучения – в 8 семестре.

Требования к «входным» знаниям, умениям и навыкам обучающегося, необходимым для освоения дисциплины: структуры данных, алгоритмы обработки информации, знание основ структурного и процедурного программирования, умение работать с логическими операторами, умение работать с циклами, массивами, строками, файлами.

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	28
Семинары, практические занятия	16
Самостоятельная работа обучающихся (всего)	100
Зачет с оценкой	+
Экзамен	-

Для очно-заочной формы обучения

Общая трудоёмкость дисциплины составляет 4 зачётных единицы 144 часа

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	144
Контактная работа	28
Аудиторная работа (всего):	28
Лекции	10
Семинары, практические занятия	18
Самостоятельная работа обучающихся (всего)	116
Зачет с оценкой	+
Экзамен	-

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.	Тема 1. Системный анализ объекта информатизации и классификация информационных активов.	34	32	6	2	4	4	24	26
2.	Тема 2. Моделирование угроз безопасности информации и формирование модели нарушителя.	34	32	6	2	4	4	24	26
3.	Тема 3. Разработка комплексной системы защиты информации	30	32	6	2	2	4	22	26

	(КСЗИ): организационные и инженерно-технические меры.								
4.	Тема 4. Обеспечение защиты информации при использовании технологий виртуализации и облачных вычислений	30	30	6	2	2	2	22	26
5.	Тема 5. Оценка эффективности системы защиты и экономический анализ затрат на информационную безопасность.	26	27	2	1	2	2	22	24
6.	Тема 6. Аттестация объектов информатизации и сопровождение жизненного цикла КСЗИ.	26	27	2	1	2	2	22	24
	Всего по дисциплине	144	144	28	10	16	18	100	116
	Контроль	-	-						
	Итого	144	144						

4.2. Содержание дисциплины, структурированное по темам (разделам)

Тема 1. Системный анализ объекта информатизации и классификация информационных активов Раскрывается методология обследования предприятия как единого целого для целей защиты информации. Изучаются методы инвентаризации материальных (серверы, рабочие станции, носители) и нематериальных (базы данных, интеллектуальная собственность, бизнес-процессы) активов. Рассматривается присвоение категорий значимости информации согласно требованиям регуляторов (например, приказы ФСТЭК России №17, №21). Анализируется понятие «контур безопасности» и границы объекта информатизации. Практическая часть включает построение схемы потоков данных внутри организации и определение точек их пересечения с недоверенной средой.

Тема 2. Моделирование угроз безопасности информации и формирование модели нарушителя Детально рассматривается процесс идентификации потенциальных опасностей в соответствии с Методикой определения актуальных угроз (ФСТЭК). Изучается классификация нарушителей по уровню потенциала (от случайного нарушителя до высококвалифицированной группировки), типу доступа (внутренний/внешний) и мотивации. Раскрывается взаимосвязь между уязвимостями системы, источниками угроз и возможными последствиями реализации атак. Студенты учатся составлять матрицу актуальности угроз и формировать профиль нарушителя, который ложится в основу технического задания на систему защиты.

Тема 3. Разработка комплексной системы защиты информации (КСЗИ): организационные и инженерно-технические меры Изучается архитектура эшелонированной («луковой») защиты. Раскрываются требования к подсистемам: *Управление доступом*: проектирование ролевых моделей (RBAC) и политик парольной защиты. *Сетевая безопасность*: сегментация сети, настройка межсетевых экранов и систем обнаружения вторжений. *Физическая защита*: контроль периметра, СКУД, видеонаблюдение, защита от утечек по техническим каналам (ПЭМИН). *Антивирусная защита и криптография*: политики использования средств шифрования и электронной подписи. Рассматривается принцип избыточности разнородных мер: если одна подсистема отказывает, другие должны компенсировать угрозу.

Тема 4. Обеспечение защиты информации при использовании технологий виртуализации и облачных вычислений Анализируются специфические риски современных ИТ-инфраструктур. Раскрываются угрозы «побега из виртуальной машины», атаки на гипервизор и проблемы изоляции ресурсов в многопользовательских средах. Изучаются средства защиты виртуальных сред (*Virtualization Security Appliances*) и микросегментация трафика внутри облака. Рассматриваются вопросы разделения ответственности (*Shared Responsibility Model*) между организацией-потребителем и провайдером облачных услуг (*IaaS, PaaS, SaaS*), а также методы контроля конфигураций (*CSPM*) и шифрования данных в облаке собственными ключами (*BYOK*).

Тема 5. Оценка эффективности системы защиты и экономический анализ затрат на информационную безопасность Раскрываются методики количественной и качественной оценки уровня защищенности. Изучаются классические показатели: ожидаемые годовые потери (*ALE — Annual Loss Expectancy*), рентабельность инвестиций в ИБ (*ROSI — Return on Security Investment*) и совокупная стоимость владения системой (*TCO*). Рассматриваются методы тестирования на проникновение (*Penetration Testing*) и инструменты анализа уязвимостей (*Vulnerability Assessment*) для проверки адекватности принятых мер реальным угрозам. Цель темы — научить обосновывать бюджет службы ИБ перед руководством компании через язык финансовых рисков.

Тема 6. Аттестация объектов информатизации и сопровождение жизненного цикла КСЗИ Изучается нормативно-правовой порядок подтверждения соответствия системы защиты установленным требованиям. Детально разбирается процедура аттестации: от подачи заявки во ФСТЭК/ФСБ до получения «Аттестата соответствия». Рассматриваются этапы приемо-сдаточных испытаний, программа и методика аттестационных испытаний. Особое внимание уделяется эксплуатации КСЗИ: управление инцидентами, плановое обслуживание средств защиты, управление изменениями (*Change Management*) и необходимость перепроектирования системы при изменении архитектуры ИТ-инфраструктуры или законодательства.

4.3. Содержание практических занятий (очная форма обучения)

Разделы, темы, дидактические единицы
Тема 1. Системный анализ объекта информатизации и классификация информационных активов Раскрывается методология обследования предприятия как единого целого для целей защиты информации. Изучаются методы инвентаризации материальных (серверы, рабочие станции, носители) и нематериальных (базы данных, интеллектуальная собственность, бизнес-процессы) активов. Рассматривается присвоение категорий значимости информации согласно требованиям регуляторов (например, приказы ФСТЭК России №17, №21).
Тема 2. Моделирование угроз безопасности информации и формирование модели нарушителя Детально рассматривается процесс идентификации потенциальных опасностей в соответствии с Методикой определения актуальных угроз (ФСТЭК). Изучается классификация нарушителей по уровню потенциала (от случайного нарушителя до высококвалифицированной группировки), типу доступа (внутренний/внешний) и мотивации.
Тема 3. Разработка комплексной системы защиты информации (КСЗИ): организационные и инженерно-технические меры Изучается архитектура эшелонированной («луковой») защиты. Раскрываются требования к подсистемам: <i>Управление доступом</i> : проектирование ролевых моделей (RBAC) и политик парольной защиты. <i>Сетевая безопасность</i> : сегментация сети, настройка межсетевых экранов и систем обнаружения вторжений. <i>Физическая защита</i> : контроль периметра, СКУД, видеонаблюдение, защита от утечек по техническим каналам (ПЭМИН).

Тема 4. Обеспечение защиты информации при использовании технологий виртуализации и облачных вычислений Анализируются специфические риски современных ИТ-инфраструктур. Раскрываются угрозы «побега из виртуальной машины», атаки на гипервизор и проблемы изоляции ресурсов в многопользовательских средах. Изучаются средства защиты виртуальных сред (<i>Virtualization Security Appliances</i>) и микросегментация трафика внутри облака.
Тема 5. Оценка эффективности системы защиты и экономический анализ затрат на информационную безопасность Раскрываются методики количественной и качественной оценки уровня защищенности. Изучаются классические показатели: ожидаемые годовые потери (<i>ALE — Annual Loss Expectancy</i>), рентабельность инвестиций в ИБ (<i>ROSI — Return on Security Investment</i>) и совокупная стоимость владения системой (<i>TCO</i>).
Тема 6. Аттестация объектов информатизации и сопровождение жизненного цикла КСЗИ Изучается нормативно-правовой порядок подтверждения соответствия системы защиты установленным требованиям. Детально разбирается процедура аттестации: от подачи заявки во ФСТЭК/ФСБ до получения «Аттестата соответствия». Рассматриваются этапы приемо-сдаточных испытаний, программа и методика аттестационных испытаний.

4.4. Содержание самостоятельной работы

Разделы, темы, дидактические единицы
Тема 1. Системный анализ объекта информатизации и классификация информационных активов Анализируется понятие «контур безопасности» и границы объекта информатизации. Практическая часть включает построение схемы потоков данных внутри организации и определение точек их пересечения с недоверенной средой.
Тема 2. Моделирование угроз безопасности информации и формирование модели нарушителя. Раскрывается взаимосвязь между уязвимостями системы, источниками угроз и возможными последствиями реализации атак. Студенты учатся составлять матрицу актуальности угроз и формировать профиль нарушителя, который ложится в основу технического задания на систему защиты.
Тема 3. Разработка комплексной системы защиты информации (КСЗИ): организационные и инженерно-технические меры <i>Антивирусная защита и криптография:</i> политики использования средств шифрования и электронной подписи. Рассматривается принцип избыточности разнородных мер: если одна подсистема отказывает, другие должны компенсировать угрозу.
Тема 4. Обеспечение защиты информации при использовании технологий виртуализации и облачных вычислений Рассматриваются вопросы разделения ответственности (<i>Shared Responsibility Model</i>) между организацией-потребителем и провайдером облачных услуг (<i>IaaS, PaaS, SaaS</i>), а также методы контроля конфигураций (<i>CSPM</i>) и шифрования данных в облаке собственными ключами (<i>BYOK</i>).
Тема 5. Оценка эффективности системы защиты и экономический анализ затрат на информационную безопасность Рассматриваются методы тестирования на проникновение (<i>Penetration Testing</i>) и инструменты анализа уязвимостей (<i>Vulnerability Assessment</i>) для проверки адекватности принятых мер реальным угрозам. Цель темы — научить обосновывать бюджет службы ИБ перед руководством компании через язык финансовых рисков.
Тема 6. Аттестация объектов информатизации и сопровождение жизненного цикла КСЗИ Эксплуатация КСЗИ: управление инцидентами, плановое обслуживание средств защиты, управление изменениями (<i>Change Management</i>) и необходимость перепроектирования системы при изменении архитектуры ИТ-инфраструктуры или законодательства.

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.

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. Глод, О. Д. Теория информационных процессов и систем : учебное пособие / О. Д. Глод. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2023. — 120 с. — ISBN 978-5-9275-4586-5. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/145115/details> (дата обращения: 22.01.2026). — Режим доступа: для авторизир. пользователей

2. 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

б) дополнительная литература:

3. Виртуализация сетевых функций и устройств : учебное пособие / М. В. Галицкий, В. А. Докучаев, В. В. Маклачкова [и др.] ; под редакцией В. А. Докучаева. — Москва : Ай Пи Ар Медиа, 2026. — 202 с. — ISBN 978-5-4497-5581-0. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/162005/details> (дата обращения: 22.01.2026). — DOI: <https://doi.org/10.23682/162005>. — Режим доступа: для авторизир. пользователей

4. Юсупов, Р. Х. Основы автоматизированных систем управления технологическими процессами : учебное пособие / Р. Х. Юсупов. — 2-е изд. — Москва, Вологда : Инфра-Инженерия, 2025. — 132 с. — ISBN 978-5-9729-2607-7. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/154724/details> (дата обращения: 22.01.2026). — 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.