

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:

fd935d10451b860e912264c0378f8448452bfdb693f94388008e29877a6bcbf5

**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

Защита информации в центрах обработки данных

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 «Защита информации в центрах обработки данных» 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.03	Защита информации в центрах обработки данных
Цель изучения дисциплины	формирование у студентов профессиональных компетенций, необходимых для обеспечения комплексной безопасности критически важной ИТ-инфраструктуры. Дисциплина направлена на изучение специфических угроз и методов защиты именно той среды, где данные не просто передаются, а хранятся и обрабатываются в огромных масштабах
Место дисциплины в структуре ОПОП	Дисциплина относится к обязательной части блока 1. «Дисциплины (модули)» программы бакалавриата
Компетенции, формируемые в результате освоения дисциплины	ПК-5, ПК-6
Содержание дисциплины	Тема 1. Физическая безопасность и инженерная защита территории ЦОД. Тема 2. Защита от утечки информации по техническим каналам (ПЭМИН). Тема 3. Сетевая архитектура безопасности и микросегментация трафика внутри ЦОД. Тема 4. Безопасность систем хранения данных (СХД) и обеспечение целостности резервных копий. Тема 5. Обеспечение информационной безопасности платформ виртуализации и облачных сред. Тема 6. Мониторинг событий ИБ, расследование инцидентов и планирование непрерывности бизнеса (BCP/DRP).
Общая трудоемкость дисциплины	Общая трудоемкость дисциплины составляет 6 зачетные единицы (216 часов)
Форма промежуточной аттестации	Зачет/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. 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
	15

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

Цель изучения дисциплины «Защита информации в центрах обработки данных» – формирование у студентов профессиональных компетенций, необходимых для обеспечения комплексной безопасности критически важной ИТ-инфраструктуры. Дисциплина направлена на изучение специфических угроз и методов защиты именно той среды, где данные не просто передаются, а хранятся и обрабатываются в огромных масштабах.

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
ПК-6	Способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными	ПК-6.1. Знает правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях, нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, нормативные методические документы ФСБ России, ФСТЭК России в области защиты информации; ПК-6.2. Владеет навыками организации и обеспечения режима секретности

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина Б1.В.03 «Защита информации в центрах обработки данных» относится к обязательной части блока 1. «Дисциплины (модули)» учебного плана ОПОП бакалавриата по направлению подготовки 10.03.02 «Информационная безопасность». Дисциплина «Принципы организации локальных вычислительных сетей» изучается обучающимися очной формы обучения в 3-4 семестре, очно-заочной формы обучения – в 3-4 семестре.

Знания, умения и навыки, полученные при изучении дисциплины «Защита информации в центрах обработки данных», будут необходимы для углубленного и осмысленного восприятия дисциплин: Операционные системы 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 6 зачетных единицы (з.е.), 216 академических часа.

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

Для очной формы обучения

Общая трудоёмкость дисциплины составляет 6 зачётных единицы 216 часа

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	216
Контактная работа	52
Аудиторная работа (всего):	52
Лекции	18
Семинары, практические занятия	34
Самостоятельная работа обучающихся (всего)	128
Курсовая работа	-
Зачет	+
Экзамен	36

Для очно-заочной формы обучения

Общая трудоёмкость дисциплины составляет 6 зачётных единиц 216 часа

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	216
Контактная работа	40
Аудиторная работа (всего):	40
Лекции	20
Семинары, практические занятия	20
Самостоятельная работа обучающихся (всего)	140
Курсовая работа	-
Зачет	+
Экзамен	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)

те	Наименование темы	Всего	Количество часов
-----------	--------------------------	--------------	-------------------------

		ОФО	ОЗФО	Контактная работа				Внеаудит. работа	
				Лекции		Практические		Самост. работа	
				ОФО	ОЗФО	ОФО	ОЗФО	ОФО	ОЗФО
1.	Тема 1. Физическая безопасность и инженерная защита территории ЦОД.	34	34	2	2	4	2	28	30
2.	Тема 2. Защита от утечки информации по техническим каналам (ПЭМИН).	34	34	4	2	4	2	28	30
3.	Тема 3. Сетевая архитектура безопасности и микросегментация трафика внутри ЦОД.	34	34	4	2	4	2	28	30
4.	Тема 4. Безопасность систем хранения данных (СХД) и обеспечение целостности резервных копий.	34	32	4	1	4	1	28	30
5.	Тема 5. Обеспечение информационной безопасности платформ виртуализации и облачных сред.	32	32	4	1	4	1	28	30
6.	Тема 6. Мониторинг событий ИБ, расследование инцидентов и планирование непрерывности бизнеса (BCP/DRP).	36	30	6	2	6	2	24	26
	Всего по дисциплине	180	180	18	20	34	20	128	140
	Контроль	36	36						
	Итого	216	216						

4.2. Содержание дисциплины, структурированное по темам (разделам)

Тема 1. Физическая безопасность и инженерная защита территории ЦОД

Раскрывается концепция защиты «периметра внутрь». Изучаются требования к размещению дата-центров, конструкции зданий (отсутствие окон в залах, укрепленные стены), системы контроля и управления доступом (СКУД) с биометрической идентификацией. Рассматриваются меры по защите от техногенных угроз: системы газового пожаротушения, прецизионное кондиционирование, организация бесперебойного электропитания (ИБП, дизель-генераторы) и заземления для предотвращения выхода оборудования из строя.

Тема 2. Защита от утечки информации по техническим каналам (ПЭМИН)

Анализируются специфические угрозы перехвата данных через побочные электромагнитные излучения и наводки. Изучается физическая природа излучений работающего компьютерного оборудования и линий связи. Рассматриваются методы противодействия: экранирование помещений серверных («клетка Фарадея»),

виброакустическая шумоизоляция ограждающих конструкций, магнитодинамическое экранирование сетей питания и использование сертифицированных пассивных средств защиты на узлах обработки конфиденциальной информации.

Тема 3. Сетевая архитектура безопасности и микросегментация трафика внутри ЦОД Изучается построение защищенной сетевой инфраструктуры дата-центра. Раскрываются принципы зонирования сети (разделение уровней доступа, распределения и ядра), изоляция управляющего трафика (*Out-of-Band Management*) от пользовательского. Особое внимание уделяется микросегментации на уровне гипервизоров и контейнеров, использованию технологий *VXLAN* для создания изолированных наложенных сетей (*Overlay*) и применению межсетевых экранов нового поколения (*NGFW*) для фильтрации трафика типа *East-West* (между серверами внутри одного зала).

Тема 4. Безопасность систем хранения данных (СХД) и обеспечение целостности резервных копий Рассматриваются методы защиты информации непосредственно на дисковых массивах и ленточных библиотеках. Изучается полнодисковое шифрование (*SED — Self-Encrypting Drives*) и программное шифрование томов СХД, управление жизненным циклом ключей шифрования. Анализируется защита протоколов блочного и файлового доступа (*iSCSI, FC, NFS*). Отдельно рассматривается стратегия защиты бэкапов: правило «3-2-1», изоляция резервных копий от основной сети (*Air Gap*) и проверка их восстанавливаемости.

Тема 5. Обеспечение информационной безопасности платформ виртуализации и облачных сред Детально разбираются риски компрометации гипервизоров (*VMware ESXi, Microsoft Hyper-V, KVM*) и платформ оркестрации (*OpenStack, Kubernetes*). Изучаются механизмы защиты плоскости управления (*Management Plane*), настройка изоляции между виртуальными машинами, предотвращение атак типа *VM Escape*. Рассматривается модель совместного разделения ответственности (*Shared Responsibility Model*) при использовании услуг коммерческих ЦОД или облаков (*IaaS/PaaS*).

Тема 6. Мониторинг событий ИБ, расследование инцидентов и планирование непрерывности бизнеса (BCP/DRP) Раскрывается роль централизованного сбора логов со всех систем ЦОД (серверы, сеть, СКУД, видеонаблюдение) в *SIEM-системах*. Изучаются сценарии типовых атак на дата-центры и алгоритмы реагирования на них. Рассматриваются методики оценки рисков доступности, проектирование катастрофоустойчивых решений (Geo-кластеризация, зеркалирование данных между площадками), разработка планов аварийного восстановления (*Disaster Recovery Plan*) и проведение регулярных тренировок персонала по отработке отказов критических узлов.

4.3. Содержание практических занятий (очная форма обучения)

Тема 1. Физическая безопасность и инженерная защита территории ЦОД Раскрывается концепция защиты «периметра внутрь». Изучаются требования к размещению дата-центров, конструкции зданий (отсутствие окон в залах, укрепленные стены), системы контроля и управления доступом (СКУД) с биометрической идентификацией.
Тема 2. Защита от утечки информации по техническим каналам (ПЭМИН) Анализируются специфические угрозы перехвата данных через побочные электромагнитные излучения и наводки. Изучается физическая природа излучений работающего компьютерного оборудования и линий связи.
Тема 3. Сетевая архитектура безопасности и микросегментация трафика внутри ЦОД Изучается построение защищенной сетевой инфраструктуры дата-центра. Раскрываются принципы зонирования сети (разделение уровней доступа, распределения и ядра), изоляция управляющего трафика (<i>Out-of-Band Management</i>) от

пользовательского.
Тема 4. Безопасность систем хранения данных (СХД) и обеспечение целостности резервных копий Рассматриваются методы защиты информации непосредственно на дисковых массивах и ленточных библиотеках. Изучается полнодисковое шифрование (<i>SED — Self-Encrypting Drives</i>) и программное шифрование томов СХД, управление жизненным циклом ключей шифрования.
Тема 5. Обеспечение информационной безопасности платформ виртуализации и облачных сред Детально разбираются риски компрометации гипервизоров (<i>VMware ESXi, Microsoft Hyper-V, KVM</i>) и платформ оркестрации (<i>OpenStack, Kubernetes</i>). Изучаются механизмы защиты плоскости управления (<i>Management Plane</i>), настройка изоляции между виртуальными машинами, предотвращение атак типа <i>VM Escape</i> .
Тема 6. Мониторинг событий ИБ, расследование инцидентов и планирование непрерывности бизнеса (BCP/DRP) Раскрывается роль централизованного сбора логов со всех систем ЦОД (серверы, сеть, СКУД, видеонаблюдение) в <i>SIEM-системах</i> . Изучаются сценарии типовых атак на дата-центры и алгоритмы реагирования на них. Рассматриваются методики оценки рисков доступности, проектирование катастрофоустойчивых решений (Гео-кластеризация, зеркалирование данных между площадками)

4.4. Содержание самостоятельной работы

Тема 1. Физическая безопасность и инженерная защита территории ЦОД Меры по защите от техногенных угроз: системы газового пожаротушения, прецизионное кондиционирование, организация бесперебойного электропитания (ИБП, дизель-генераторы) и заземления для предотвращения выхода оборудования из строя.
Тема 2. Защита от утечки информации по техническим каналам (ПЭМИН) Методы противодействия: экранирование помещений серверных («клетка Фарадея»), виброакустическая зашумление ограждающих конструкций, магнитодинамическое зашумление сетей питания и использование сертифицированных пассивных средств защиты на узлах обработки конфиденциальной информации.
Тема 3. Сетевая архитектура безопасности и микросегментация трафика внутри ЦОД Микросегментация на уровне гипервизоров и контейнеров, использованию технологий <i>VXLAN</i> для создания изолированных наложенных сетей (<i>Overlay</i>) и применению межсетевых экранов нового поколения (<i>NGFW</i>) для фильтрации трафика типа <i>East-West</i> (между серверами внутри одного зала).
Тема 4. Безопасность систем хранения данных (СХД) и обеспечение целостности резервных копий Стратегия защиты бэкапов: правило «3-2-1», изоляция резервных копий от основной сети (<i>Air Gap</i>) и проверка их восстанавливаемости.
Тема 5. Обеспечение информационной безопасности платформ виртуализации и облачных сред Модель совместного разделения ответственности (<i>Shared Responsibility Model</i>) при использовании услуг коммерческих ЦОД или облаков (<i>IaaS/PaaS</i>).
Тема 6. Мониторинг событий ИБ, расследование инцидентов и планирование непрерывности бизнеса (BCP/DRP) Разработка планов аварийного восстановления (<i>Disaster Recovery Plan</i>) и проведение регулярных тренировок персонала по отработке отказов критических узлов.

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. Томилов, И. Н. Информационные сети. Основы проектирования сетей : учебное пособие / И. Н. Томилов, Е. Е. Истратова. — Новосибирск : Новосибирский государственный технический университет, 2023. — 68 с. — ISBN 978-5-7782-4890-8. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/155408/details> (дата обращения: 27.01.2026). — Режим доступа: для авторизир. пользователей

2. Мельников, А. В. Основы информационной безопасности : учебное пособие / А. В. Мельников, С. В. Зарубин. — Москва : Российский государственный университет правосудия имени В.М. Лебедева, 2025. — 220 с. — ISBN 978-5-00209-188-1. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/152309/details> (дата обращения: 27.01.2026). — Режим доступа: для авторизир. пользователей

б) дополнительная литература:

3. Уймин, А. Г. Компьютерные сети. L2-технологии : практикум для СПО / А. Г. Уймин. — Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2024. — 190 с. — ISBN 978-5-4497-2559-2, 978-5-4488-1745-8. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/135231/details> (дата обращения: 27.01.2026). — DOI: <https://doi.org/10.23682/135231>. — Режим доступа: для авторизир. пользователей

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.