

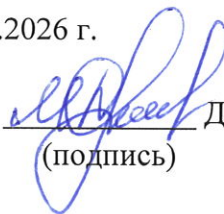


Рабочая программа составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки 09.03.01 "Информатика и вычислительная техника", утвержденного приказом Министерства науки и высшего образования Российской Федерации от 19.09.2017 №929 (зарегистрировано в Министерстве юстиции РФ 10.10.2017 №48489) с изменениями и дополнениями.

Программу составил старший преподаватель Яковенко Л.В.

Рабочая программа дисциплины «Безопасность компьютерных сетей» утверждена на заседании кафедры «Управление и бизнес-информатика».

Протокол № 6 от 29.01.2026 г.

Заведующий кафедрой  Д.В. Моторина  
(подпись)

<b>АННОТАЦИЯ</b>	
Индекс дисциплины по учебному плану	Наименование дисциплины
<b>Б1.О.32</b>	<b>БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ</b>
Цель изучения дисциплины	формирование у обучающихся знаний в области обеспечения безопасности компьютерных сетей и навыков практического обеспечения защиты информации и безопасного использования программных и аппаратных средств в сетях.
Место дисциплины в структуре ОПОП	Дисциплина Безопасность компьютерных сетей относится к базовой части ОПОП и является обязательной для освоения.
Компетенции, формируемые в результате освоения дисциплины	ОПК-4, ОПК-7
Содержание дисциплины	Тема 1. Введение в безопасность компьютерных сетей Тема 2. Принципы построения защищенных сетей Тема 3. Угрозы и риски в компьютерных сетях Тема 4. Методы и механизмы защиты компьютерных сетей Тема 5. Управление безопасностью и мониторинг сети Тема 6. Современные тенденции и перспективные направления в обеспечении безопасности
Общая трудоемкость дисциплины	Общая трудоемкость дисциплины составляет 4 зачетные единицы (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

Целью преподавания дисциплины «Безопасность компьютерных сетей» является формирование у обучающихся знаний в области обеспечения безопасности компьютерных сетей и навыков практического обеспечения защиты информации и безопасного использования программных и аппаратных средств в сетях.

Основная задача состоит в том, чтобы студенты освоили принципы комплексного подхода к вопросам безопасности, научились анализировать потенциальные угрозы и выявлять риски безопасности, а также познакомились с современными методами и средствами защиты информации в компьютерных сетях.

Кроме того, дисциплина направлена на ознакомление студентов с основными положениями нормативно-правовой базы в области информационной безопасности, такими как требования к защите корпоративных информационных систем от несанкционированного доступа, скрытых воздействий и утечек информации по техническим каналам.

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 участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1. Знать: основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. ОПК-4.2. Уметь: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. ОПК-4.3. Владеть: составлением технической документации на различных этапах жизненного цикла информационной системы
ОПК-7	Способен участвовать в настройке и наладке программно-аппаратных комплексов	ОПК-7.1. Знать: методы настройки, наладки программно-аппаратных комплексов. ОПК-7.2. Уметь: анализировать техническую документацию, производить настройку, наладку и тестирование программно-аппаратных комплексов. ОПК-7.3. Владеть: навыками проверки работоспособности программно-аппаратных комплексов

## 2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина Безопасность компьютерных сетей относится к базовой части ОПОП и является обязательной для освоения, изучается обучающимися очной формы обучения в 7 семестре, очно-заочной формы обучения – в 7 семестре.

Дисциплина является базовой для освоения дисциплин Компьютерные вирусы, CASE-средства проектирования.

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

##### Для очной формы обучения

Общая трудоемкость дисциплины составляет 4 зачётных единицы 144 часа

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	144
Контактная работа	44
Аудиторная работа (всего):	44
Лекции	16
Семинары, практические занятия	28
Самостоятельная работа обучающихся (всего)	100
Курсовая работа	-
Зачет с оценкой	+

##### Для очно-заочной формы обучения

Общая трудоемкость 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
Курсовая работа	-
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 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. Введение в безопасность компьютерных сетей	28	26	4	2	6	4	18	20
2.	Тема 2. Принципы построения защищенных сетей	28	26	4	2	6	4	18	20
3.	Тема 3. Угрозы и риски в компьютерных сетях	22	26	2	2	4	4	16	20
4.	Тема 4. Методы и механизмы защиты компьютерных сетей	22	24	2	2	4	2	16	20
5.	Тема 5. Управление безопасностью и мониторинг сети	22	21	2	1	4	2	16	18
6.	Тема 6. Современные тенденции и перспективные направления в обеспечении безопасности	22	21	2	1	4	2	16	18
	Всего по дисциплине	<b>144</b>	<b>144</b>	<b>16</b>	<b>10</b>	<b>28</b>	<b>18</b>	<b>100</b>	<b>116</b>
	Контроль	-	-						
	<b>Итого</b>	<b>144</b>	<b>144</b>						

#### 4.2. Содержание дисциплины, структурированное по темам (разделам)

Разделы, темы, дидактические единицы
<p><b>Тема 1. Введение в безопасность компьютерных сетей</b></p> <p><b>Терминология:</b> защита информации, угроза, атака, уязвимости, атаки DoS/DDoS, перехват пакетов, взлом паролей.</p> <p><b>История развития:</b> этапы эволюции сетевой безопасности от простых мер защиты до современных подходов.</p> <p><b>Современные проблемы:</b> растущие объемы кибератак, переход на удаленную работу и новые типы угроз.</p>
<p><b>Тема 2. Принципы построения защищенных сетей</b></p> <p>Вторая тема посвящена изучению общих архитектурных принципов и подходов к созданию защищенных компьютерных сетей. Здесь рассматриваются:</p> <p>Стандарты и протоколы обеспечения безопасности (например, TLS, IPsec, VPN).</p> <p>Политики безопасности и контроль доступа (ACL, аутентификация пользователей).</p> <p>Шифрование данных и защита каналов передачи.</p> <p>Разделение зон ответственности и уровней доверия в сети.</p>
<p><b>Тема 3. Угрозы и риски в компьютерных сетях</b></p> <p>Третья тема фокусируется на типовых угрозах и рисках, возникающих в компьютерные сети, и способах их минимизации. Включены такие аспекты, как:</p> <p>Атаки на доступность (DoS/DDoS).</p> <p>Уязвимости веб-приложений (XSS, CSRF, SQL injection).</p> <p>Способы обнаружения и нейтрализации вредоносного ПО.</p> <p>Анализ риска проникновения злоумышленника и его последствий.</p>

<p><b>Тема 4. Методы и механизмы защиты компьютерных сетей</b>  Четвертая тема детально рассматривает конкретные методы и инструменты защиты сетей. Рассматриваются:  Межсетевые экраны (Firewall): политика фильтрации, NAT, прокси-серверы.  Антивирусные системы и обнаружение вторжений (IDS/IPS).  Мониторинг активности сети и выявление подозрительного поведения.  Контроль целостности данных и логирование действий пользователей.</p>
<p><b>Тема 5. Управление безопасностью и мониторинг сети</b>  Пятая тема сосредоточена на управлении безопасностью сети и процессах мониторинга текущих угроз. Тематика включает:  Планирование и реализация стратегии безопасности предприятия.  Оценка уровня защищенности сети (аудит безопасности).  Реакция на инциденты безопасности и постатаковая реабилитация.  Регулярные аудиты и тестирование на проникновение («penetration testing»).</p>
<p><b>Тема 6. Современные тенденции и перспективные направления в обеспечении безопасности</b>  Биометрия и мультифакторная аутентификация.  Искусственный интеллект и машинное обучение в обнаружении угроз.  Облачная инфраструктура и ее влияние на защиту данных.  Прогнозирование будущих угроз и разработка превентивных мер.</p>

### 4.3. Содержание практических занятий (очная форма обучения)

Разделы, темы, дидактические единицы
<p><b>Тема 1. Введение в безопасность компьютерных сетей</b>  <b>Терминология:</b> защита информации, угроза, атака, уязвимости, атаки DoS/DDoS, перехват пакетов, взлом паролей.  <b>История развития:</b> этапы эволюции сетевой безопасности от простых мер защиты до современных подходов.</p>
<p><b>Тема 2. Принципы построения защищенных сетей</b>  Вторая тема посвящена изучению общих архитектурных принципов и подходов к созданию защищенных компьютерных сетей. Здесь рассматриваются:  Стандарты и протоколы обеспечения безопасности (например, TLS, IPsec, VPN).  Политики безопасности и контроль доступа (ACL, аутентификация пользователей).</p>
<p><b>Тема 3. Угрозы и риски в компьютерных сетях</b>  Третья тема фокусируется на типовых угрозах и рисках, возникающих в компьютерные сети, и способах их минимизации. Включены такие аспекты, как:  Атаки на доступность (DoS/DDoS).  Уязвимости веб-приложений (XSS, CSRF, SQL injection).</p>
<p><b>Тема 4. Методы и механизмы защиты компьютерных сетей</b>  Четвертая тема детально рассматривает конкретные методы и инструменты защиты сетей. Рассматриваются:  Межсетевые экраны (Firewall): политика фильтрации, NAT, прокси-серверы.  Антивирусные системы и обнаружение вторжений (IDS/IPS).</p>
<p><b>Тема 5. Управление безопасностью и мониторинг сети</b>  Пятая тема сосредоточена на управлении безопасностью сети и процессах мониторинга текущих угроз. Тематика включает:  Планирование и реализация стратегии безопасности предприятия.</p>

**Тема 6. Современные тенденции и перспективные направления в обеспечении безопасности**  
 Биометрия и мультифакторная аутентификация.  
 Искусственный интеллект и машинное обучение в обнаружении угроз.  
 Облачная инфраструктура и ее влияние на защиту данных.

#### 4.4. Содержание самостоятельной работы

Разделы, темы, дидактические единицы
<p><b>Тема 1. Введение в безопасность компьютерных сетей</b>  <b>Современные проблемы:</b> растущие объемы кибератак, переход на удаленную работу и новые типы угроз.</p>
<p><b>Тема 2. Принципы построения защищенных сетей</b>            Шифрование данных и защита каналов передачи.            Разделение зон ответственности и уровней доверия в сети.</p>
<p><b>Тема 3. Угрозы и риски в компьютерных сетях</b>            Способы обнаружения и нейтрализации вредоносного ПО.            Анализ риска проникновения злоумышленника и его последствий.</p>
<p><b>Тема 4. Методы и механизмы защиты компьютерных сетей</b>            Мониторинг активности сети и выявление подозрительного поведения.            Контроль целостности данных и логирование действий пользователей.</p>
<p><b>Тема 5. Управление безопасностью и мониторинг сети</b>            Оценка уровня защищенности сети (аудит безопасности).            Реакция на инциденты безопасности и постатаковая реабилитация.            Регулярные аудиты и тестирование на проникновение («penetration testing»).</p>
<p><b>Тема 6. Современные тенденции и перспективные направления в обеспечении безопасности</b>            Прогнозирование будущих угроз и разработка превентивных мер.</p>

#### 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. Технологии защиты информации в компьютерных сетях : учебное пособие для СПО / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суоров. — 2-е изд. — Саратов : Профобразование, 2024. — 368 с. — ISBN 978-5-4488-1014-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/139767.html> (дата обращения: 27.05.2025). — Режим доступа: для авторизир. пользователей

2. Технологии защиты информации в компьютерных сетях : учебное пособие / Н.А. Руденков [и др.]. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2025. — 368 с. — ISBN 978-5-4497-0931-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/146404.html> (дата обращения: 26.04.2025). — Режим доступа: для авторизир. пользователей

**б) дополнительная литература:**

3. Куликов, С. С. Информационная безопасность локальных компьютерных сетей : практикум / С. С. Куликов. — Воронеж : Воронежский государственный технический университет, ЭБС АСВ, 2021. — 57 с. — ISBN 978-5-7731-0969-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/118614.html> (дата обращения: 01.04.2025). — Режим доступа: для авторизир. пользователей

4. Урбанович, П. П. Компьютерные сети : учебное пособие / П. П. Урбанович, Д. М. Романенко. — Москва, Вологда : Инфра-Инженерия, 2022. — 460 с. — ISBN 978-5-9729-0962-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/124197.html> (дата обращения: 01.07.2025). — 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 учебного кабинета:

- 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.

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