

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

fd935d10451b860e912264c0378f8448452b693f94388008e29877a6bcbf5

**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

Безопасность беспроводных локальных сетей

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 В.Л. Мазниченко, старший преподаватель

Рабочая программа дисциплины «Безопасность беспроводных локальных сетей» 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.03.01	Безопасность беспроводных локальных сетей
Цель изучения дисциплины	формирование у студентов профессиональных компетенций, необходимых для проектирования, развертывания и аудита безопасности беспроводных сетей (Wi-Fi) в условиях открытой и недоверенной среды передачи данных.
Место дисциплины в структуре ОПОП	Дисциплина относится к обязательной части блока 1. «Дисциплины (модули)» программы бакалавриата
Компетенции, формируемые в результате освоения дисциплины	ПК-6
Содержание дисциплины	Тема 1. Специфика физической среды: распространение радиоволн и архитектурные особенности Wi-Fi. Тема 2. Уязвимости ранних стандартов защиты: WEP, WPA и TKIP. Тема 3. Современная защита корпоративных сетей: стандарт WPA2/WPA3 и AES. Тема 4. Протоколы аутентификации и инфраструктура управления доступом: 802.1X, RADIUS, EAP. Тема 5. Типовые атаки на беспроводные сети и методы противодействия. Тема 6. Безопасность специализированных режимов: гостевые сети, Hotspot 2.0 (Passpoint) и IoT.
Общая трудоемкость дисциплины	Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 часов)
Форма промежуточной аттестации	Зачет

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 «Безопасность беспроводных локальных сетей» – формирование у студентов профессиональных компетенций, необходимых для проектирования, развертывания и аудита безопасности беспроводных сетей (Wi-Fi) в условиях открытой и недоверенной среды передачи данных.

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-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 Безопасность беспроводных локальных сетей относится к обязательной части блока 1. «Дисциплины (модули)» учебного плана ОПОП бакалавриата по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина «Безопасность беспроводных локальных сетей» изучается обучающимися очной формы обучения в 6 семестре, очно-заочной формы обучения – в 6 семестре.

Знания, умения и навыки, полученные при изучении дисциплины «Безопасность беспроводных локальных сетей», будут необходимы для углубленного и осмысленного восприятия дисциплин: Системное программирование, Алгоритмизация и программирование 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 3 зачетных единицы (з.е.), 108 академических часа.

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

Для очной формы обучения

Общая трудоёмкость дисциплины составляет 3 зачётных единицы 108 часа

Объём дисциплины	Всего часов
Общая трудоёмкость дисциплины	108
Контактная работа	38
Аудиторная работа (всего):	38
Лекции	12
Семинары, практические занятия	26
Самостоятельная работа обучающихся (всего)	70
Зачет	+

Для очно-заочной формы обучения

Общая трудоёмкость дисциплины составляет 3 зачётных единицы 108 часа

Объём дисциплины	Всего часов
Общая трудоёмкость дисциплины	108
Контактная работа	28
Аудиторная работа (всего):	28
Лекции	10
Семинары, практические занятия	18
Самостоятельная работа обучающихся (всего)	80
Зачет	-

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. Специфика физической среды: распространение радиоволн и архитектурные особенности Wi-Fi.	6	6	2	2	-	-	4	4
2.	Тема 2. Уязвимости ранних стандартов защиты: WEP, WPA и TKIP.	12	12	2	2	2	-	8	10
3.	Тема 3. Современная защита корпоративных сетей: стандарт	12	12	2	2	2	2	8	8

	WPA2/WPA3 и AES.								
4.	Тема 4. Протоколы аутентификации и инфраструктура управления доступом: 802.1X, RADIUS, EAP.	20	20	2	1	14	10	4	9
5.	Тема 5. Типовые атаки на беспроводные сети и методы противодействия.	12	12	2	1	4	4	6	9
6.	Тема 6. Безопасность специализированных режимов: гостевые сети, Hotspot 2.0 (Passpoint) и IoT.	10	10	2	2	4	4	4	4
	Всего по дисциплине	108	108	12	10	26	18	70	80
	Контроль	-	-						
	Итого	108	108						

4.2. Содержание дисциплины, структурированное по темам (разделам)

Тема 1. Специфика физической среды: распространение радиоволн и архитектурные особенности Wi-Fi Раскрываются физические основы работы беспроводных сетей: диапазоны частот 2,4 ГГц и 5/6 ГГц, влияние препятствий на сигнал, зоны Френеля. Изучается архитектура IEEE 802.11: режимы BSS (инфраструктурный), IBSS (Ad-Hoc) и ESS. Рассматриваются риски неконтролируемого распространения сигнала за пределы охраняемой территории офиса («RF-Leakage»).

Тема 2. Уязвимости ранних стандартов защиты: WEP, WPA и TKIP Анализируются критические ошибки протоколов первого поколения. Подробно разбирается атака FMS на алгоритм шифрования RC4 в протоколе WEP, позволяющая вычислить секретный ключ за считанные минуты. Изучается уязвимость протокола временной целостности ключей (TKIP) к атакам типа QoS-манипуляция и инъекции пакетов (Mikhail exploit).

Тема 3. Современная защита корпоративных сетей: стандарт WPA2/WPA3 и AES Изучается механизм работы блочного шифра AES в режиме счетчика (CCMP), который пришел на смену потоковым шифрам. Разбирается четырехстороннее рукопожатие (4-Way Handshake) для генерации динамических сессионных ключей. Особое внимание уделяется новому стандарту WPA3: индивидуальной защите кадров (Individual Data Protection) и устойчивости к офлайн-атакам по словарю благодаря методу SAE (Simultaneous Authentication of Equals).

Тема 4. Протоколы аутентификации и инфраструктура управления доступом: 802.1X, RADIUS, EAP Рассматривается переход от общих паролей (PSK) к персональной идентификации пользователей. Изучается работа стандарта IEEE 802.1X: роли Supplicant (клиент), Authenticator (точка доступа) и Authentication Server (RADIUS-сервер). Анализируются методы расширяемого протокола аутентификации (EAP): сертификаты (EAP-TLS), туннелирование (PEAP, EAP-TTLS) и их применимость в корпоративном сегменте.

Тема 5. Типовые атаки на беспроводные сети и методы противодействия Систематизируются угрозы: Атаки типа «человек посередине» (Evil Twin, Karma) — создание поддельной точки доступа для перехвата данных. Отказ в обслуживании

(*Deauthentication/Disassociation flood*) — принудительный разрыв соединений легитимных клиентов. Пассивное сканирование и сбор хендшейков для последующего брутфорса пароля. Изучаются средства защиты: системы обнаружения вторжений в беспроводные сети (*Wireless IDS*), использование белых списков MAC-адресов и изоляции клиентов на уровне L2.

Тема 6. Безопасность специализированных режимов: гостевые сети, Hotspot 2.0 (Passpoint) и IoT Рассматриваются технологии безопасного предоставления интернета посетителям без ущерба для внутренней сети (использование VLAN и контроллеров WLC). Изучается специфика защищенного подключения мобильных устройств через протокол *Hotspot 2.0* (автоматическая аутентификация по SIM-карте). Анализируются проблемы безопасности устройств интернета вещей (*IoT*), не поддерживающих современные стандарты WPA, и способы их изолированного подключения.

4.3. Содержание практических занятий (очная форма обучения)

Тема 1. Специфика физической среды: распространение радиоволн и архитектурные особенности Wi-Fi Раскрываются физические основы работы беспроводных сетей: диапазоны частот 2.4 ГГц и 5/6 ГГц, влияние препятствий на сигнал, зоны Френеля. Изучается архитектура IEEE 802.11: режимы BSS (инфраструктурный), IBSS (<i>Ad-Hoc</i>) и ESS.
Тема 2. Уязвимости ранних стандартов защиты: WEP, WPA и TKIP Анализируются критические ошибки протоколов первого поколения. Подробно разбирается атака FMS на алгоритм шифрования RC4 в протоколе WEP, позволяющая вычислить секретный ключ за считанные минуты.
Тема 3. Современная защита корпоративных сетей: стандарт WPA2/WPA3 и AES Изучается механизм работы блочного шифра AES в режиме счетчика (CCMP), который пришел на смену потоковым шифрам. Разбирается четырехстороннее рукопожатие (<i>4-Way Handshake</i>) для генерации динамических сессионных ключей.
Тема 4. Протоколы аутентификации и инфраструктура управления доступом: 802.1X, RADIUS, EAP Рассматривается переход от общих паролей (PSK) к персональной идентификации пользователей. Изучается работа стандарта IEEE 802.1X: роли Supplicant (клиент), Authenticator (точка доступа) и Authentication Server (RADIUS-сервер).
Тема 5. Типовые атаки на беспроводные сети и методы противодействия Систематизируются угрозы: Атаки типа «человек посередине» (<i>Evil Twin, Karma</i>) — создание поддельной точки доступа для перехвата данных. Отказ в обслуживании (<i>Deauthentication/Disassociation flood</i>) — принудительный разрыв соединений легитимных клиентов. Пассивное сканирование и сбор хендшейков для последующего брутфорса пароля.
Тема 6. Безопасность специализированных режимов: гостевые сети, Hotspot 2.0 (Passpoint) и IoT Рассматриваются технологии безопасного предоставления интернета посетителям без ущерба для внутренней сети (использование VLAN и контроллеров WLC). Изучается специфика защищенного подключения мобильных устройств через протокол <i>Hotspot 2.0</i> (автоматическая аутентификация по SIM-карте).

4.4. Содержание самостоятельной работы

Тема 1. Специфика физической среды: распространение радиоволн и архитектурные особенности Wi-Fi Рассматриваются риски неконтролируемого
--

распространения сигнала за пределы охраняемой территории офиса («RF-Leakage»).
Тема 2. Уязвимости ранних стандартов защиты: WEP, WPA и TKIP Изучается уязвимость протокола временной целостности ключей (TKIP) к атакам типа <i>QoS-манипуляция</i> и инъекции пакетов (<i>Mikhail exploit</i>).
Тема 3. Современная защита корпоративных сетей: стандарт WPA2/WPA3 и AES Особое внимание уделяется новому стандарту WPA3: индивидуальной защите кадров (<i>Individual Data Protection</i>) и устойчивости к офлайн-атакам по словарю благодаря методу <i>SAE (Simultaneous Authentication of Equals)</i> .
Тема 4. Протоколы аутентификации и инфраструктура управления доступом: 802.1X, RADIUS, EAP Анализируются методы расширяемого протокола аутентификации (EAP): сертификаты (<i>EAP-TLS</i>), туннелирование (<i>PEAP, EAP-TTLS</i>) и их применимость в корпоративном сегменте.
Тема 5. Типовые атаки на беспроводные сети и методы противодействия Средства защиты: системы обнаружения вторжений в беспроводные сети (<i>Wireless IDS</i>), использование белых списков MAC-адресов и изоляции клиентов на уровне L2.
Тема 6. Безопасность специализированных режимов: гостевые сети, Hotspot 2.0 (Passpoint) и IoT Анализируются проблемы безопасности устройств интернета вещей (<i>IoT</i>), не поддерживающих современные стандарты WPA, и способы их изолированного подключения.

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 – 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. Бабаев, С. И. Компьютерные сети. Ч.2. Глобальные и беспроводные сети : учебник / С. И. Бабаев, Б. В. Костров, М. Б. Никифоров. — Москва : КУРС, 2024. — 160 с. — ISBN 978-5-907064-23-2. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/144794/details> (дата обращения: 27.01.2026). — Режим доступа: для авторизир. пользователей

2. Беленький, В. Г. Беспроводные сети передачи данных : учебное пособие для СПО / В. Г. Беленький, А. В. Лошкарев. — Саратов : Профобразование, 2022. — 98 с. — ISBN 978-5-4488-1499-0. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/125572/details> (дата обращения: 27.01.2026). — DOI: <https://doi.org/10.23682/125572>. — Режим доступа: для авторизир. пользователей

б) дополнительная 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

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: ноутбук с лицензионным программным обеспечением и возможностью подключения к информационно-телекоммуникационной сети Интернет; мультимедийная установка; наглядные пособия.

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