

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Узунов Федор Владимирович

Должность: Ректор

Дата подписания: 30.09.2026 09:20:01

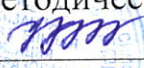
Уникальный программный ключ:

fd935d10451b860e912264c0378f8448452b6db603f94388008e20877a6bcbf5

**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

Разработка защищенного программного обеспечения

Направление подготовки

10.03.01 «Информационная безопасность»

Профиль

Безопасность компьютерных систем

Квалификация выпускника

Бакалавр

Для всех

форм обучения

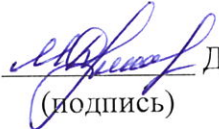
Симферополь, 2026

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 «Разработка защищенного программного обеспечения» 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.08	Разработка защищенного программного обеспечения
Цель изучения дисциплины	формирование у студентов профессиональных компетенций, необходимых для создания программных продуктов и систем, устойчивых к преднамеренным атакам. Дисциплина направлена на изучение методологии безопасного жизненного цикла разработки ПО (<i>Secure SDLC</i>) и освоение практических навыков выявления и устранения уязвимостей на всех этапах — от проектирования архитектуры до эксплуатации.
Место дисциплины в структуре ОПОП	Дисциплина относится к обязательной части блока 1. «Дисциплины (модули)» программы бакалавриата
Компетенции, формируемые в результате освоения дисциплины	ПК-4
Содержание дисциплины	Тема 1. Методология безопасной разработки (<i>Secure SDLC</i>) и моделирование угроз. Тема 2. Безопасное проектирование архитектур и паттерны защиты. Тема 3. Уязвимости языков программирования и методы их нейтрализации (C/C++, Java, Python). Тема 4. Защита веб-приложений и противодействие инъекциям (OWASP Top 10). Тема 5. Методы анализа защищенности исходного кода: SAST, DAST и фаззинг. Тема 6. Криптографическая защита данных в приложениях и защита от реверс-инжиниринга
Общая трудоемкость дисциплины	Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 часов)
Форма промежуточной аттестации	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

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

Цель изучения дисциплины «Разработка защищенного программного обеспечения» – формирование у студентов профессиональных компетенций, необходимых для создания программных продуктов и систем, устойчивых к преднамеренным атакам. Дисциплина направлена на изучение методологии безопасного жизненного цикла разработки ПО (*Secure SDLC*) и освоение практических навыков выявления и устранения уязвимостей на всех этапах — от проектирования архитектуры до эксплуатации.

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-4	Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	ПК-4.1. Знает свойства, функции и признаки документа, в том числе как объекта нападения и защиты; основы документационного обеспечения управления, задачи органов защиты информации на предприятиях, порядок организации работы и нормативные правовые акты по сертификации средств защиты информации; ПК-4.2. Умеет квалифицированно исследовать состав документации предприятия (организации), разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; владеет методами формирования требований по защите информации

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина Б1.В.08 «Разработка защищенного программного обеспечения» относится к обязательной части блока 1. «Дисциплины (модули)» учебного плана ОПОП бакалавриата по направлению подготовки 10.03.02 «Информационная безопасность». Дисциплина «Разработка защищенного программного обеспечения» изучается обучающимися очной формы обучения в 6 семестре, очно-заочной формы обучения – в 6 семестре.

Знания, умения и навыки, полученные при изучении дисциплины «Разработка защищенного программного обеспечения», будут необходимы для углубленного и осмысленного восприятия дисциплин: Информатика и основы программирования, 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 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)	34
Курсовая работа	-
Зачет	-
Экзамен	36

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)	44
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 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. Методология безопасной разработки (Secure SDLC) и моделирование угроз.	6	6	2	2	-	-	4	4

2.	Тема 2. Безопасное проектирование архитектур и паттерны защиты.	12	12	2	2	2	-	8	10
3.	Тема 3. Уязвимости языков программирования и методы их нейтрализации (C/C++, Java, Python).	12	12	2	2	2	2	8	8
4.	Тема 4. Защита веб-приложений и противодействие инъекциям (OWASP Top 10).	20	20	2	1	14	10	4	9
5.	Тема 5. Методы анализа защищенности исходного кода: SAST, DAST и фаззинг.	12	12	2	1	4	4	6	9
6.	Тема 6. Криптографическая защита данных в приложениях и защита от реверс-инжиниринга	10	10	2	2	4	4	4	4
	Всего по дисциплине	72	72	12	10	26	18	34	44
	Контроль	36	36						
	Итого	108	108						

4.2. Содержание дисциплины, структурированное по темам (разделам)

Тема 1. Методология безопасной разработки (Secure SDLC) и моделирование угроз Раскрывается концепция интеграции безопасности в каждый этап жизненного цикла ПО (*Requirements, Design, Implementation, Testing, Maintenance*). Изучается процесс построения формализованной модели угроз (например, по методике *STRIDE*) и дерева атак (*Attack Trees*). Рассматривается экономическая целесообразность раннего обнаружения дефектов («стоимость исправления ошибки растет экспоненциально»).

Тема 2. Безопасное проектирование архитектур и паттерны защиты Изучаются принципы минимизации поверхности атаки, эшелонированной обороны (*Defense in Depth*) и наименьших привилегий. Анализируются архитектурные решения для изоляции компонентов (микросервисы, контейнеризация), безопасное хранение секретов (вне исходного кода) и использование шаблонов проектирования, таких как централизованная проверка входных данных и отказоустойчивая обработка исключений.

Тема 3. Уязвимости языков программирования и методы их нейтрализации (C/C++, Java, Python) Детально рассматриваются типичные ошибки работы с памятью: переполнение буфера стека и кучи, целочисленные переполнения, использование памяти после освобождения (*Use-After-Free*). Для управляемых языков изучаются проблемы десериализации недоверенных данных, утечки через логирование чувствительной информации и небезопасное управление сессиями. Даются рекомендации по использованию безопасных аналогов стандартных функций.

Тема 4. Защита веб-приложений и противодействие инъекциям (OWASP Top 10) Анализируются наиболее критические риски безопасности веба. Глубоко разбирается природа атак типа *SQL Injection*, *XSS (Cross-Site Scripting)*, *CSRF (Cross-Site Request Forgery)* и *Broken Access Control*. Изучаются методы защиты: строгая параметризация запросов, контекстный вывод данных, использование современных заголовков безопасности (*Content Security Policy*, *HttpOnly/SameSite cookies*) и механизмов анти-CSRF токенов.

Тема 5. Методы анализа защищенности исходного кода: SAST, DAST и фаззинг Рассматриваются инструменты автоматизации поиска уязвимостей. Изучается статический анализ (SAST) — поиск дефектов без запуска программы (анализ абстрактного синтаксического дерева). Раскрываются основы динамического анализа (DAST) и фаззинга (*Fuzzing*) — подачи случайных входных данных для вызова сбоев во время выполнения. Сравниваются подходы «белого», «черного» и «серого» ящика при тестировании.

Тема 6. Криптографическая защита данных в приложениях и защита от реверс-инжиниринга Изучаются правила корректного использования готовых криптопримитивов: выбор стойких алгоритмов шифрования (AES-GCM), режимов работы, генерация случайных чисел и надежное хранение ключей (Key Management). Отдельно рассматривается безопасность мобильного и десктопного ПО: техники обфускации кода, контроль целостности бинарных файлов (*Code Signing*) и защита от отладки/декомпиляции для предотвращения кражи интеллектуальной собственности.

4.3. Содержание практических занятий (очная форма обучения)

Тема 1. Методология безопасной разработки (Secure SDLC) и моделирование угроз Раскрывается концепция интеграции безопасности в каждый этап жизненного цикла ПО (<i>Requirements, Design, Implementation, Testing, Maintenance</i>). Изучается процесс построения формализованной модели угроз (например, по методике <i>STRIDE</i>) и дерева атак (<i>Attack Trees</i>).
Тема 2. Безопасное проектирование архитектур и паттерны защиты Изучаются принципы минимизации поверхности атаки, эшелонированной обороны (<i>Defense in Depth</i>) и наименьших привилегий. Анализируются архитектурные решения для изоляции компонентов (микросервисы, контейнеризация).
Тема 3. Уязвимости языков программирования и методы их нейтрализации (C/C++, Java, Python) Детально рассматриваются типичные ошибки работы с памятью: переполнение буфера стека и кучи, целочисленные переполнения, использование памяти после освобождения (<i>Use-After-Free</i>).
Тема 4. Защита веб-приложений и противодействие инъекциям (OWASP Top 10) Анализируются наиболее критические риски безопасности веба. Глубоко разбирается природа атак типа <i>SQL Injection, XSS (Cross-Site Scripting), CSRF (Cross-Site Request Forgery)</i> и <i>Broken Access Control</i> .
Тема 5. Методы анализа защищенности исходного кода: SAST, DAST и фаззинг Рассматриваются инструменты автоматизации поиска уязвимостей. Изучается статический анализ (SAST) — поиск дефектов без запуска программы (анализ абстрактного синтаксического дерева).
Тема 6. Криптографическая защита данных в приложениях и защита от реверс-инжиниринга Изучаются правила корректного использования готовых криптопримитивов: выбор стойких алгоритмов шифрования (AES-GCM), режимов работы, генерация случайных чисел и надежное хранение ключей (Key Management).

4.4. Содержание самостоятельной работы

Тема 1. Методология безопасной разработки (Secure SDLC) и моделирование угроз Экономическая целесообразность раннего обнаружения дефектов («стоимость исправления ошибки растет экспоненциально»).
Тема 2. Безопасное проектирование архитектур и паттерны защиты Безопасное

хранение секретов (вне исходного кода) и использование шаблонов проектирования, таких как централизованная проверка входных данных и отказоустойчивая обработка исключений.
Тема 3. Уязвимости языков программирования и методы их нейтрализации (C/C++, Java, Python) Проблемы десериализации недоверенных данных, утечки через логирование чувствительной информации и небезопасное управление сессиями. Даются рекомендации по использованию безопасных аналогов стандартных функций.
Тема 4. Защита веб-приложений и противодействие инъекциям (OWASP Top 10) Методы защиты: строгая параметризация запросов, контекстный вывод данных, использование современных заголовков безопасности (<i>Content Security Policy</i> , <i>HttpOnly/SameSite cookies</i>) и механизмов анти-CSRF токенов.
Тема 5. Методы анализа защищенности исходного кода: SAST, DAST и фаззинг Основы динамического анализа (DAST) и фаззинга (Fuzzing) — подачи случайных входных данных для вызова сбоев во время выполнения. Сравняются подходы «белого», «черного» и «серого» ящика при тестировании.
Тема 6. Криптографическая защита данных в приложениях и защита от реверс-инжиниринга Безопасность мобильного и десктопного ПО: техники обфускации кода, контроль целостности бинарных файлов (<i>Code Signing</i>) и защита от отладки/декомпиляции для предотвращения кражи интеллектуальной собственности.

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. Башмакова, Е. И. Информатика и информационные технологии. Технология работы в MS WORD 2016 : учебное пособие / Е. И. Башмакова. — Москва : Ай Пи Ар Медиа, 2020. — 90 с. — ISBN 978-5-4497-0515-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/94204.html> (дата обращения: 16.01.2026). — Режим доступа: для авторизир. пользователей.

2. Фот, Ю. Д. Анализ уязвимостей и защита программного обеспечения : практикум / Ю. Д. Фот, Е. И. Ларионова. — Оренбург : Оренбургский государственный университет, ЭБС АСВ, 2025. — 141 с. — ISBN 978-5-7410-3391-3. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/153174/details> (дата обращения: 27.01.2026). — Режим доступа: для авторизир. пользователей

б) дополнительная литература:

3. 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.