



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И.
Носова»



УТВЕРЖДАЮ
Директор ИЭиАС
В.Р. Храмынин

04.02.2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

***ОСНОВЫ БЕЗОПАСНОЙ РАЗРАБОТКИ ПРОГРАММНОГО
ОБЕСПЕЧЕНИЯ***

Направление подготовки (специальность)
09.04.01 Информатика и вычислительная техника

Направленность (профиль/специализация) программы
Программное обеспечение для цифровизации предприятий и организаций

Уровень высшего образования - магистратура

Форма обучения
очная

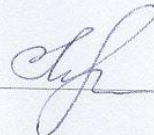
Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Вычислительной техники и программирования
Курс	2
Семестр	3

Магнитогорск
2025 год

Рабочая программа составлена на основе ФГОС ВО - магистратура по направлению подготовки 09.04.01 Информатика и вычислительная техника (приказ Минобрнауки России от 19.09.2017 г. № 918)

Рабочая программа рассмотрена и одобрена на заседании кафедры
Вычислительной техники и программирования
03.02.2025 г, протокол № 5

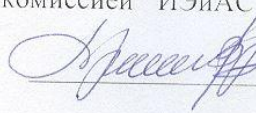
Зав. кафедрой



О.С. Логунова

Рабочая программа одобрена методической комиссией ИЭиАС
04.02.2025 г. протокол № 3

Председатель



В.Р. Храмшин

Рабочая программа составлена:
доцент кафедры ВТиП, канд. техн. наук



Ю.В. Кочержинская

Рецензент:

директор НИИ «Промбезопасность», д-р техн. наук



М.Ю. Наркевич

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2026 - 2027 учебном году на заседании кафедры Вычислительной техники и программирования

Протокол от ____ 20__ г. № ____
Зав. кафедрой _____ О.С. Логунова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2027 - 2028 учебном году на заседании кафедры Вычислительной техники и программирования

Протокол от ____ 20__ г. № ____
Зав. кафедрой _____ О.С. Логунова

1 Цели освоения дисциплины (модуля)

Дисциплина "Основы безопасной разработки программного обеспечения" посвящена безопасному программированию. Внедрение мер по разработке безопасного программного обеспечения (ПО) на всех этапах жизненного цикла является обязательным условием конкурентоспособности на рынке для компаний, занимающихся разработкой ПО. Цель дисциплины – дать представление о полном цикле разработки безопасного программного обеспечения. Для достижения поставленной цели, решаются следующие задачи:

- формирование базиса знаний, позволяющего понимать принципы безопасного программирования;
- анализировать статические и динамические угрозы безопасности;
- выбирать средства и технологии разработки;
- оценивать риски информационной безопасности.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Основы безопасной разработки программного обеспечения входит в обязательную часть учебного плана образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Современные проблемы цифровизации предприятий и организаций

Методы и средства высокопроизводительного программирования

Интеллектуальные системы

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Выполнение и защита выпускной квалификационной работы

Подготовка к сдаче и сдача государственного экзамена

Oracle Database: продвинутые аспекты программирования и настройки производительности

Проблемы принятия решений в условиях нечеткой информации

Производственная - технологическая (проектно-технологическая) практика

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Основы безопасной разработки программного обеспечения» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ОПК-5	Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем;
ОПК-5.1	Определяет необходимость и участвует в разработке и модернизации программного и аппаратного обеспечение информационных и автоматизированных систем
ОПК-6	Способен разрабатывать компоненты программно-аппаратных комплексов обработки информации и автоматизированного проектирования;
ОПК-6.1	Определяет необходимость в разработке компонент программно-аппаратных комплексов обработки информации и автоматизированного проектирования

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 4 зачетных единиц 144 акад. часов, в том числе:

- контактная работа – 37,15 акад. часов;
- аудиторная – 34 акад. часов;
- внеаудиторная – 3,15 акад. часов;
- самостоятельная работа – 71,15 акад. часов;
- в форме практической подготовки – 0 акад. час;
- подготовка к экзамену – 35,7 акад. час

Форма аттестации - экзамен

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Основные методологии SSDLC (Secure software development lifecycle, жизненный цикл безопасной разработки)								
1.1 Современное устройство SDLC & SSDLC. Участники и роли SDLC & SSDLC. Принципы и требования SSDLC. Этапы SSDLC. Практики SSDLC & Agile.	3	2	4		10	Подготовка к выполнению лабораторной работе.	Дискуссия. Проверка выполнения лабораторной работы.	ОПК-5.1, ОПК-6.1
1.2 Международные и отечественные стандарты в области SSDLC. Практика их применения в процессе разработки. ГОСТ Р 56939-2016., OWASP Top10, NIST, MITRE, Zero trust security model.		3	4		15	Подготовка к выполнению лабораторной работе.	Дискуссия. Проверка выполнения лабораторной работы.	ОПК-5.1, ОПК-6.1
1.3 Требования безопасности согласно SSDLC на каждом из этапов разработки ПО)		4	4		11,15	Подготовка к выполнению лабораторной работе.	Дискуссия. Проверка выполнения лабораторной работы.	ОПК-5.1, ОПК-6.1
Итого по разделу		9	12		36,15			
2. Методы оценки надежности и защищенности информационных систем								
2.1 Требования безопасности согласно этапам SSDLC. Моделирование угроз. Инструменты	3	4	2		20	Подготовка к выполнению лабораторной работе.	Дискуссия. Проверка выполнения лабораторной работы.	ОПК-5.1, ОПК-6.1

автоматизации процесса (Threat Dragon, Irius Risk, Microsoft threat modeling tool). Статический анализ. Sast-плагины для сред разработки. Динамический анализ, Fuzzing.								
2.2 Анализ программных компонентов, SBOM. Ревью кода.	3	2	2		10	Подготовка к выполнению лабораторной работе.	Дискуссия. Проверка выполнения лабораторной работы.	ОПК-5.1, ОПК-6.1
2.3 Язык моделирования CORAS как инструмент описания угроз, уязвимостей, инцидентов и активов, а также взаимосвязей между ними. Моделирование сценариев угроз при разработке ПО.		2	1		5	Подготовка к выполнению лабораторной работе.	Дискуссия. Проверка выполнения лабораторной работы.	ОПК-5.1, ОПК-6.1
Итого по разделу		8	5		35			
3. Экзамен								
3.1 Экзамен	3					Подготовка к экзамену	Экзамен	ОПК-5.1, ОПК-6.1
Итого по разделу								
Итого за семестр		17	17		71,15		экзамен	
Итого по дисциплине		17	17		71,15		экзамен	

5 Образовательные технологии

1. Традиционные образовательные технологии, ориентированные на организацию образовательного процесса и предполагающую прямую трансляцию знаний от преподавателя к студенту.

Формы учебных занятий с использованием традиционных технологий:

Информационная лекция – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя).

Лабораторная работа – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

2. Технологии проблемного обучения – организация образовательного процесса, которая предполагает постановку проблемных вопросов, создание учебных проблемных ситуаций для стимулирования активной познавательной деятельности студентов.

3. Интерактивные технологии – организация образовательного процесса, которая предполагает активное и нелинейное взаимодействие всех участников, достижение на этой основе лично значимого для них образовательного результата.

Формы учебных занятий с использованием специализированных интерактивных технологий:

Лекция «обратной связи» – лекция–провокация (изложение материала с заранее запланированными ошибками), лекция-беседа, лекция-дискуссия, лекция-конференция.

4. Информационно-коммуникационные образовательные технологии – организация образовательного процесса, основанная на применении программных сред и технических средств работы со знаниями в различных предметных областях.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины

а) Основная литература:

1. Казарин, О. В. Надежность и безопасность программного обеспечения : учебник для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2025. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/563862> (дата обращения: 08.04.2025). — Режим доступа: по подписке.

2. Криптографическая защита информации : учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.] ; под ред. С.О. Крамарова. — Москва : РИОР : ИНФРА-М, 2023. — 321 с. — (Высшее образование). — DOI: <https://doi.org/10.12737/1716-6>. - ISBN 978-5-369-01716-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1899016> (дата обращения: 24.04.2024). — Режим доступа: по подписке.

б) Дополнительная литература:

1. Поддержка принятия решений при проектировании систем защиты информации : монография / В.В. Бухтояров, М.Н. Жукова, В.В. Золотарев [и др.]. — Москва : ИНФРА-М, 2020. — 131 с. — (Научная мысль). — www.dx.doi.org/10.12737/2248. - ISBN 978-5-16-009519-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1036519> (дата обращения: 08.04.2025). — Режим доступа: по подписке.

2. Хоффман Эндрю. Безопасность веб-приложений. Разведка, защита, нападение. 2-е изд. - Астана : Спринт Бук, 2025. - 432 с. - ISBN 978-601-08-4270-0. - URL: <https://ibooks.ru/bookshelf/397516/reading> (дата обращения: 08.04.2025). - Текст: электронный. — Режим доступа: по подписке.

в) Методические указания:

1. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2025. — 355 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: <https://doi.org/10.29039/01848-4>. - ISBN 978-5-369-01969-6. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2173934> (дата обращения: 08.04.2025). — Режим доступа: по подписке.

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
FlowVision	К-93-09 от 19.06.2009	бессрочно
Borland Turbo C++	№112301 от 23.11.2005	бессрочно
Eclipse	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

1. Лекционная аудитория ауд. 282. Мультимедийные средства хранения, передачи и представления информации.

2. Компьютерные классы Центра информационных технологий ФГБОУ ВО «МГТУ». Персональные компьютеры, объединенные в локальные сети с выходом в Internet, оснащенные современными программно-методическими комплексами для решения задач в области информатики и вычислительной техники.

3. Аудитории для самостоятельной работы: компьютерные классы; читальные залы библиотеки. Все классы УИТ и АСУ с персональными компьютерами, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

4. Аудиторий для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Ауд. 282 и классы УИТ и АСУ.

5. Помещения для самостоятельной работы обучающихся, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и наличием доступа в электронную информационно-образовательную среду организации. Классы УИТ и АСУ.

6. Помещения для хранения и профилактического обслуживания учебного оборудования. Центр информационных технологий – ауд. 372

Приложение 1

Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Основы безопасной разработки программного обеспечения» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа студентов предполагает выполнение лабораторных работ.

Лабораторные работы находятся в электронном источнике:

1. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2025. — 355 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: <https://doi.org/10.29039/01848-4>. - ISBN 978-5-369-01969-6. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2173934> (дата обращения: 08.04.2025). – Режим доступа: по подписке..

Приложение 2

Оценочные средства для проведения промежуточной аттестации

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Код индикатора	Индикатор достижения компетенции	Оценочные средства
ОПК-5: Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем;		
ОПК-5.1	Определяет необходимость и участвует в разработке и модернизации программного и аппаратного обеспечение информационных и автоматизированных систем	Характеристика шифра, определяющая стойкость шифра к дешифрованию без знания ключа, называется 1) криптостойкостью 2) надежностью 3) эффективностью 4) уровнем безопасности
		Что позволяет предотвратить использование криптографических преобразований: 1) отказ от информации; 2) обеспечение аутентификации; 3) утечку информации; 4) использование алгоритмов асимметричного шифрования.
		Ниже перечислены механизмы защиты информационных систем от несанкционированного доступа. Что здесь лишнее: 1) идентификация и аутентификация пользователей и субъектов доступа; 2) управление доступом; 3) обеспечение постоянного числа пользователей сети; 4) обеспечения целостности; 5) регистрация и учет.
ОПК-6: Способен разрабатывать компоненты программно-аппаратных комплексов обработки информации и автоматизированного проектирования;		
ПК-6.1	Определяет необходимость в разработке компонент программно-аппаратных комплексов обработки информации и автоматизированного проектирования	Какой из режимов алгоритма DES используется для построения шифров гаммирования? 1) электронная кодовая книга; 2) сцепление блоков шифра; 3) обратная связь по шифротексту; 4) обратная связь по выходу.
		Что означает «многократное шифрование» применительно к блочным шифрам: 1) повторное применение алгоритма шифрования к шифротексту с теми же ключами; 2) шифрование одного и того же блока открытого текста несколько раз с несколькими ключами; 3) повторное применение алгоритма шифрования к шифротексту с другими ключами; 4) увеличение числа этапов шифрования открытого текста.
		Укажите разницу между SDLC и STLC: 1) SDLC предполагает полную проверку и валидацию проекта, тогда как STLC предполагает только

валидацию;

2) STLC предполагает полную проверку и валидацию проекта, тогда как SDLC предполагает только валидацию;

3) оба ответа неверны.

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Промежуточная аттестация по дисциплине «Основы безопасной разработки программного обеспечения» включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме экзамена изучения дисциплины.

Экзамен по дисциплине проводится в устной форме по билетам.

Показатели и критерии оценивания экзамена:

– на оценку **«отлично»** – обучающийся показывает высокий уровень сформированности компетенций, т.е. полно раскрыто содержание материала; чётко и правильно даны определения и раскрыто содержание материала; ответ самостоятельный, при ответе использованы знания, приобретённые ранее;

– на оценку **«хорошо»** – обучающийся показывает средний уровень сформированности компетенций, т.е. раскрыто основное содержание материала в объёме; в основном правильно даны определения, понятия; материал изложен неполно, при ответе допущены неточности, нарушена последовательность изложения; допущены небольшие неточности при выводах и использовании терминов; практические навыки нетвёрдые;

– на оценку **«удовлетворительно»** – обучающийся показывает пороговый уровень сформированности компетенций, т.е. усвоено основное содержание материала, но изложено фрагментарно, не всегда последовательно; определения и понятия даны не чётко; практические навыки слабые;

– на оценку **«неудовлетворительно»** – результат обучения не достигнут, обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач.