

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ

Ректор Белорусского
государственного университета

А.Д.Король



26 мая 2025 г.

Регистрационный № УД-14108/уч.

НЕФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Учебная программа учреждения образования по учебной дисциплине для
специальности:

1-31 03 07 Прикладная информатика (по направлениям)

Направление специальности:

**1-31 03 07-01 Прикладная информатика (программное обеспечение
компьютерных систем)**

2025 г.

Учебная программа составлена на основе ОСВО 1-31 03 07-2021 и учебного плана № G31-1-216/уч. от 22.03.2022.

СОСТАВИТЕЛИ:

Д.М.Кульчавый, старший преподаватель кафедры вычислительной математики факультета прикладной математики и информатики Белорусского государственного университета;

П.А.Мандрик, доцент кафедры вычислительной математики факультета прикладной математики и информатики Белорусского государственного университета, кандидат физико-математических наук, доцент;

В.И.Репников, заведующий кафедрой вычислительной математики факультета прикладной математики и информатики Белорусского государственного университета, кандидат физико-математических наук, доцент

РЕЦЕНЗЕНТ:

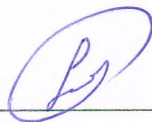
М.С.Стенин, заместитель директора ООО «Траектория качества»

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой вычислительной математики БГУ
(протокол № 13 от 15.05.2025);

Научно-методическим советом БГУ
(протокол № 10 от 22.05.2025)

Заведующий кафедрой



В.И.Репников

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная дисциплина «Нефункциональное тестирование информационных систем» посвящена изучению особенностей проектирования интерфейсов для мобильных устройств, а также основ тестирования безопасности веб-приложений на основе открытой методологии OWASP (Open Web Application Security Project).

Содержание дисциплины по уровню новизны материала отвечает современному состоянию вопроса. В результате изучения данной дисциплины студенты должны освоить основные методологии проектирования веб-интерфейсов и анализе их защищенности.

Цели и задачи учебной дисциплины

Цель учебной дисциплины «Нефункциональное тестирование информационных систем» – обучить студентов особенностям оценки юзабилити и правилам ее проведения, проектированию web-проектов, особенностям проектирования интерфейсов для мобильных устройств, оценке доступности (accessibility); обучить основам тестирования безопасности веб-приложений, а именно, анализу защищенности, на основе открытой методологии OWASP (Open Web Application Security Project); получить практические навыки выбора и использования инструментария анализа защищенности веб-приложений.

В рамках поставленных целей задачи учебной дисциплины состоят в следующем:

1. формирование у студентов практических навыков по поиску и анализу уязвимостей веб-приложений как со стороны серверной, так и клиентской частей;
2. освоение принципов определения технологического стека, используемого при разработке приложения.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием.

Учебная дисциплина относится к дисциплинам специализации (1-31 03 07-01 07 Надежность и тестирование информационных систем) компонента учреждения высшего образования.

Связи с другими учебными дисциплинами: основой для изучения данной дисциплины являются дисциплины государственного компонента модуля «Программирование».

Учебный материал, излагаемый в данной дисциплине, тесно связан с учебной дисциплиной «Управление проектами тестирования информационных систем» цикла дисциплин специализации.

Требования к компетенциям

Освоение учебной дисциплины «Управление проектами тестирования информационных систем» должно обеспечить формирование следующих компетенций:

Универсальные компетенции:

решать задачи профессиональной деятельности на основе применения информационно-коммуникационных технологий;

Специализированные компетенции:

находить и анализировать научную информацию по темам, связанным с будущей профессиональной деятельностью, с применением современных технологий поиска, обработки и анализа информации, использовать глобальные информационные ресурсы, компьютерные методы сбора, хранения и обработки информации.

В результате освоения учебной дисциплины студент должен:

знать:

- терминологию, применяемую в сфере юзабилити и проектирования опыта взаимодействия;
- основные принципы и порядок проведения оценки юзабилити;
- инструменты, используемые для проектирования web-проектов и оценки юзабилити;
- терминологию, применяемую в сфере тестирования безопасности;
- основные методологии, используемые при проведении анализа защищенности веб-приложений;
- разновидности угроз безопасности веб-приложений, методы их обнаружения;
- разновидности уязвимостей веб-приложений, отличительные особенности, возможные последствия эксплуатации.

уметь:

- проводить юзабилити-аудит;
- проводить юзабилити-тестирование;
- проектировать web-интерфейсы для десктопных и мобильных устройств;
- проводить оценку доступности интерфейса;
- различать виды тестов безопасности, необходимость и последовательность применения;
- определять уровень угрозы, классифицировать в соответствии с методикой OWASP Risk Calculation;
- производить поиск и анализ уязвимостей веб-приложений как со стороны серверной, так и клиентской частей;
- определять технологический стек (набор технологий), используемый при разработке приложения.

владеть:

- инструментарием, используемым для проектирования web-проектов и оценки юзабилити;
- техникой поиска уязвимостей приложений.

Структура учебной дисциплины

Дисциплина изучается в 7 семестре. В соответствии с учебным планом всего на изучение учебной дисциплины «Нефункциональное тестирование информационных систем» отведено для **очной формы** получения высшего образования – 200 часов, в том числе 72 аудиторных часа: лекции – 36 часов, лабораторные занятия – 36 часов. Из них:

Лекции – 36 часов, лабораторные занятия – 30 часов, управляемая самостоятельная работа (УСР) – 6 часов.

Трудоемкость учебной дисциплины составляет 6 зачетных единиц.

Форма промежуточной аттестации – зачет.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел I. Основы юзабилити и проектирования опыта взаимодействия

Тема 1.1. Основные понятия, принципы, компетенции

Понятие юзабилити и UX. Компетенции UX. Схема Джесса Гарретта. Принципы HCD.

Раздел II. Определение целевой аудитории

Тема 2.1. Определение целевой аудитории, анализ пользователей

Определение целевой аудитории, ментальные модели. Сегментация ЦА. Исследования и персонажи.

Раздел III. Оценка юзабилити

Тема 3.1. Методы оценки юзабилити

Комбинированный метод. Экспертиза компонентов. Чеклисты. Оценка по рекомендациям и стандартам. Эвристические методы. Оценка с привлечением пользователей.

Тема 3.2. Юзабилити-аудит

Эвристическая оценка. Рекомендации ведущих экспертов. Эвристики Нильсена. Влияние на пользователя. Составление отчета.

Тема 3.3. Юзабилити-тестирование от А до Я

Основные правила подбора респондентов. Преимущества и недостатки ЮТ. Виды ЮТ и роли. Планирование ЮТ. Метрики. Сценарии тестирования. Рекомендации по проведению ЮТ. Анализ результатов. Инструменты для проведения ЮТ.

Раздел IV. Создание прототипов пользовательских интерфейсов

Тема 4.1. Информационная архитектура

Понятие информационной архитектуры. Компоненты информационной архитектуры.

Тема 4.2. Основы проектирования

Элементы интерфейса. Удачные решения. Проектирование web-интерфейса. Инструменты проектирования.

Тема 4.3. Проектирование для мобильных устройств

Особенности проектирования для мобильных устройств. Проектирование мобильной версии web-интерфейса.

Раздел V. Оценка доступности (accessibility)

Тема 5.1. Принципы оценки и способы ее проведения

Принципы WCAG 2.0. Тестирование доступности. Инструменты для проведения тестирования доступности.

Раздел VI. Введение в тестирование безопасности

Тема 6.1. Терминология

Модель нарушителя. Мобильный код. Уязвимость. Угроза. Эксплуатация уязвимости. Эксплойт. Вектор атаки. Инъекция. Отказ в обслуживании. Доступность. С니ффер. Конфиденциальность данных. Защищенность. Целостность данных. Методология тестирования (OWASP, OSSTM, WASC). Стандарт безопасности. Политика безопасности. Уязвимость нулевого дня. Патч. Заплата. Сканнер безопасности.

Тема 6.2. Виды тестов

Идентификация приложения. Анализ защищенности. Тест на проникновение. Аудит безопасности. Сетевой аудит безопасности. Моделирование угроз. Статический и динамический анализ кода. Социальная инженерия.

Раздел VII. Тестирование безопасности на основе методологии OWASP

Тема 7.1. Идентификация приложения

Архитектура веб-приложения (уровень приложения, уровень данных, уровень бизнес-логики). Технологический стек. Spider. Crawler. Fingerprinting. POST и GET запросы. CVE база. Обработчик ошибки. Сканнер портов. Сниффер. Раскрытие данных.

Тема 7.2. Уязвимости клиента

Валидация данных на стороне клиента. Инъекции кода (SQL, XML, Code, ORM, Javascript, CSS, AD, SMTP). Обход валидации данных. Кросс-сайт скриптинг. DOM атака. Механизм сессий. Аутентификация и авторизация пользователя. Защищенный канал передачи данных.

Тема 7.3. Уязвимости сервера

Слабое шифрование (частная реализация криптоалгоритмов, отсутствие SSL). Атаки на отказ в обслуживании (DoS, DDoS). Переполнение буфера. Прямые ссылки на объекты. Инъекции команд операционной системы. Раскрытие конфигурационных файлов. Контроль обновления программных продуктов. Атака на консоль администратора.

Тема 7.4. Ошибки реализации бизнес логики

Защита от средств автоматизации. Условия гонки (race condition). Небезопасное восстановление данных. Горизонтальная и вертикальная эскалация прав пользователя. Противоречивость функциональных требований. Функциональные дефекты.

Тема 7.5. Средства аудита. Отслеживание изменений

Логгирование действий пользователя. Журналы операционной системы. Контрольная сумма. Хэш-функция. IDS/IPS.

Тема 7.6. Вспомогательный инструментарий

Выбор инструментария. Kali Linux – дистрибутив инженера по анализу защищенности ПО и сети. Сканнер безопасности. Псевдо-срабатывание. Анализ отчета. Недостатки автоматизированных инструментов.

Раздел VIII. Тестирование безопасности в жизненном цикле разработки программного обеспечения

Тема 8.1. Оценка риска взлома. Оценка сложности взлома

OWASP Risk Calculation. Сложность взлома. Критичность уязвимости. Определение значимости взлома. Обзор тенденций. Примеры уязвимостей и успешных атак. Комбинирование уязвимостей при построении атаки.

Тема 8.2. Внедрение тестирования безопасности в жизненный цикл разработки ПО

Формирование отчета по тестированию безопасности. Рекомендации по исправлению ошибок кода. Повторный тест безопасности. Тестовая и производственная среды. Миграция ПО в облако (риски). Контроль защищенности ПО на различных стадиях разработки и внедрения. Взаимодействие с разработчиками. Демонстрация уязвимостей. Проект по анализу защищенности веб-приложения.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Очная (дневная) форма получения высшего образования с применением
дистанционных образовательных технологий (ДОТ)

Номер раздела,	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Форма контроля
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
1	Основы юзабилити и проектирования опыта взаимодействия	2			2			
1.1	Основные понятия, принципы, компетенции	2			2			Экспресс-опрос
2	Определение целевой аудитории	2			2			
2.1	Определение целевой аудитории, анализ пользователей	2			2			Отчет по расчетно-графической работе, экспресс-опрос
3	Оценка юзабилити	6			4		2	
3.1	Методы оценки юзабилити	2			2			Экспресс-опрос
3.2	Юзабилити-аудит	2			2			Экспресс-опрос
3.3	Юзабилити-тестирование от А до Я	2					2	Отчет по расчетно-графической работе, экспресс-опрос, Контрольная работа по темам 1.1-3.3
4	Создание прототипов пользовательских интерфейсов	4			4		4	
4.1	Информационная архитектура	2						Экспресс-опрос

4.2	Основы проектирования	2			2		2	Отчет по расчетно-графической работе , экспресс-опрос
4.3	Проектирование для мобильных устройств				2		2	Экспресс-опрос
5	Оценка доступности (accessibility)	2			2			
5.1	Принципы оценки и способы ее проведения	2			2			Экспресс-опрос
6	Введение в тестирование безопасности	4			2			
6.1	Терминология	2						Экспресс-опрос
6.2	Виды тестов	2			2			Отчет по расчетно-графической работе, экспресс-опрос
7	Тестирование безопасности на основе методологии OWASP	12			10			
7.1	Идентификация приложения	2						Экспресс-опрос
7.2	Уязвимости клиента	2			2			Экспресс-опрос
7.3	Уязвимости сервера	2			2			Экспресс-опрос
7.4	Ошибки реализации бизнес логики	2			2			Экспресс-опрос
7.5	Средства аудита. Отслеживание изменений	2			2			Экспресс-опрос
7.6	Вспомогательный инструментарий	2			2			Отчет по расчетно-графической работе, экспресс-опрос, Контрольная работа по темам 4.1-7.6

8	Тестирование безопасности в жизненном цикле разработки программного обеспечения	4			4			
8.1	Оценка риска взлома. Оценка сложности взлома	2			2			Экспресс-опрос
8.2	Внедрение тестирования безопасности в жизненный цикл разработки ПО	2			2			Отчет по расчетно-графической работе, экспресс-опрос

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Основная литература

1. Голубев, А. Н. Нефункциональное тестирование программного обеспечения. – Москва: БХВ-Петербург, 2018.
2. Ямалов Р.Р. Дизайн-мышление и UX-стратегия для бизнеса. – М.: Альпина Паблишер, 2023.
3. Тимченко С.Л., Леонтьев Б.К. UX-исследования. Практическое руководство для специалистов в России. – М.: Бомбора, 2022.
4. Эрик Райс. UX-исследования. Как понять своих пользователей и создать нужный продукт. – М.: Диалектика, 2022.

Дополнительная литература

5. Бочаров, А. В., Кузнецов, С. А. Тестирование программного обеспечения: теория и практика. – Санкт-Петербург: Питер, 2019.
6. Винниченко, И. В. Автоматизация процессов тестирования. – СПб.: Питер, 2005. – с. 203.
7. Герасютин А.С. Проектирование пользовательских интерфейсов. UI/UX-дизайн и юзабилити. – СПб.: Питер, 2021.
8. Коллектив авторов под ред. Широкова Р.В. Практикум по юзабилити-тестированию веб-интерфейсов. – М.: ДМК Пресс, 2023.
9. Джефф Готтшел, Кори Линч. UX-стратегия. Как провести исследование пользователей и рынка, чтобы создавать по-настоящему востребованные цифровые продукты. – М.: Альпина Паблишер, 2022.
10. Стив Круг. Не заставляйте меня думать. – М.: Питер, 2020.
11. Якоб Нильсен, Ральф Фаранд. Мобильная юзабилити. – М.: Манн, Иванов и Фербер, 2021
12. Торрес Руссо. UX-письмо: Как создавать тексты для интерфейсов. – М.: ОДРИ, 2023.
13. Том Эррико. Доступность веб-контента: Руководство по WCAG 2.2. – М.: Логос, 2023.

Ресурсы в интернете

1. ISTQB (International Software Testing Qualifications Board) - <https://www.istqb.org>
2. Ministry of Testing - <https://www.ministryoftesting.com>
3. Software Testing Help - <https://www.softwaretestinghelp.com>

Перечень рекомендуемых средств диагностики и методика формирования итоговой отметки

Для диагностики компетенций могут использоваться следующие средства текущей аттестации: отчеты по расчетно-графическим работам, письменные контрольные работы, устные экспресс-опросы.

Расчетно-графические работы, как правило, представляют собой задания, включающие программную реализацию указанного вида работ, проведение вычислительного эксперимента и комментарии по его итогам. Рекомендуемая форма отчетности по расчетно-графической работе – письменный отчет. Расчетно-графическая работа оценивается по 10-балльной шкале. Отметка за расчетно-графическую работу может быть снижена в случае несвоевременного выполнения.

Письменные контрольные работы проводятся для контроля знаний по одному или нескольким разделам дисциплины. Они включают 4–5 заданий и оцениваются по 10-балльной шкале. В случае неудовлетворительной отметки контрольная работа может быть переписана.

Устный экспресс-опрос студентов проводится в свободной форме во время лабораторных и лекционных занятий. Его результаты учитываются преподавателем при выставлении итоговой отметки.

Формой промежуточной аттестации по дисциплине «Нефункциональное тестирование информационных систем» учебным планом предусмотрен зачёт.

Примерный перечень заданий для управляемой самостоятельной работы

Тема 3.3. Юзабилити-тестирование от А до Я (2 ч)

Примерное задание:

1. Провести экспертную оценку методом чеклистов, экспертизы компонентов.
2. Провести экспертную оценку методом экспертизы компонентов.
3. Провести экспертную оценку по эвристикам Нильсена.
4. Провести лабораторное юзабилити-тестирование.

Форма контроля: отчет по расчетно-графической работе

Тема 4.2. Основы проектирования (2 ч)

Примерное задание:

1. Создать прототип web-страницы.
2. Провести экспертную оценку существующего web-интерфейса.

Форма контроля: отчет по расчетно-графической работе

Тема 4.3. Проектирование для мобильных устройств (2 ч)

Примерное задание:

1. Создать прототип мобильной версии web-страницы.

2. Провести экспертную оценку существующего мобильного web-интерфейса.

Форма контроля: экспресс-опрос

Описание инновационных подходов и методов к преподаванию учебной дисциплины

При организации занятий используется **практико-ориентированный подход**, который предполагает:

- освоение содержания образования через решения практических задач;
- приобретение навыков эффективного выполнения разных видов профессиональной деятельности.

Также при организации образовательного процесса используется **метод группового обучения**, который представляет собой форму организации учебно-познавательной деятельности обучающихся, предполагающую функционирование разных типов малых групп, работающих как над общими, так и специфическими учебными заданиями.

Методические рекомендации по организации самостоятельной работы

Для организации самостоятельной работы студентов по учебной дисциплине следует использовать современные информационные технологии: разместить в сетевом доступе комплекс учебных и учебно-методических материалов (учебно-программные материалы, методические указания к лабораторным занятиям, материалы текущего контроля и текущей аттестации, позволяющие определить соответствие учебной деятельности обучающихся требованиям образовательных стандартов высшего образования и учебно-программной документации, в т.ч. вопросы для подготовки к зачету, экзамену, список рекомендуемой литературы, информационных ресурсов и др.). Эффективность самостоятельной работы студентов проверяется в ходе текущего и итогового контроля знаний. Для общей оценки качества усвоения студентами учебного материала рекомендуется использование рейтинговой системы.

Примерный перечень вопросов к зачету

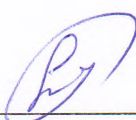
1. Понятие юзабилити-тестирования (ЮТ). Схема Джесса Гарретта.
2. Определение целевой аудитории, ментальные модели.
3. Комбинированный метод. Экспертиза компонентов. Чеклисты.
4. Оценка по рекомендациям и стандартам. Эвристические методы.
5. Оценка с привлечением пользователей. Влияние на пользователя.
6. Эвристическая оценка. Рекомендации ведущих экспертов.
7. Основные правила подбора респондентов.
8. Преимущества и недостатки ЮТ.
9. Виды ЮТ и роли. Планирование ЮТ. Метрики.
10. Сценарии тестирования. Рекомендации по проведению ЮТ.

11. Инструменты для проведения ЮТ.
12. Элементы интерфейса. Удачные решения. Проектирование web-интерфейса.
13. Особенности проектирования для мобильных устройств.
14. Виды тестов. Идентификация приложения.
15. Виды тестов. Анализ защищенности. Тест на проникновение.
16. Виды тестов. Аудит безопасности. Сетевой аудит безопасности.
17. Виды тестов. Моделирование угроз.
18. Статический и динамический анализ кода.
19. Виды тестов. Уязвимости клиента
20. Виды тестов. Уязвимости сервера
21. Ошибки реализации бизнес логики
22. Средства аудита. Отслеживание изменений
23. Вспомогательный инструментарий
24. Оценка риска взлома. Оценка сложности взлома

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УО

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Учебная дисциплина не требует согласования			

Заведующий кафедрой
вычислительной математики
доцент, кандидат физ.-мат. наук


 (подпись)

В.И.Репников

15.05.2025

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ УО

на ____ / ____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры
_____ (протокол № ____ от _____ 202_ г.)

Заведующий кафедрой

УТВЕРЖДАЮ
Декан факультета
