

**Министерство науки и высшего образования РФ**  
**Федеральное государственное бюджетное образовательное учреждение**  
**высшего образования**  
**«Национальный исследовательский университет «МЭИ»**

---

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность компьютерных систем (продвинутый уровень)

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная


**Рабочая программа дисциплины**  
**БЕЗОПАСНОСТЬ WEB-ПРИЛОЖЕНИЙ**

<b>Блок:</b>	<b>Блок 1 «Дисциплины (модули)»</b>
<b>Часть образовательной программы:</b>	<b>Часть, формируемая участниками образовательных отношений</b>
<b>№ дисциплины по учебному плану:</b>	<b>Б4.Ч.06</b>
<b>Трудоемкость в зачетных единицах:</b>	<b>7 семестр - 2;</b>
<b>Часов (всего) по учебному плану:</b>	<b>72 часа</b>
<b>Лекции</b>	<b>7 семестр - 16 часов;</b>
<b>Практические занятия</b>	<b>7 семестр - 16 часов;</b>
<b>Лабораторные работы</b>	<b>не предусмотрено учебным планом</b>
<b>Консультации</b>	<b>проводится в рамках часов аудиторных занятий</b>
<b>Самостоятельная работа</b>	<b>7 семестр - 39,7 часа;</b>
<b>в том числе на КП/КР</b>	<b>не предусмотрено учебным планом</b>
<b>Иная контактная работа</b>	<b>проводится в рамках часов аудиторных занятий</b>
<b>включая:</b>	
<b>Отчет</b>	
<b>Домашнее задание</b>	
<b>Промежуточная аттестация:</b>	
<b>Зачет</b>	<b>7 семестр - 0,3 часа;</b>

**Москва 2023**

**ПРОГРАММУ СОСТАВИЛ:**


Преподаватель

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Дратвяк А.В.
	Идентификатор	R1a0ecc29-DratviakAV-b9b11303

А.В. Дратвяк


**СОГЛАСОВАНО:**

Руководитель  
образовательной программы

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Баронов О.Р.
	Идентификатор	R90d76356-BaronovOR-7bf8fd7e

О.Р. Баронов

Заведующий выпускающей  
кафедрой

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Невский А.Ю.
	Идентификатор	R4bc65573-NevskyAY-0b6e493d

А.Ю. Невский

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**Цель освоения дисциплины:** формирование знаний о современных подходах обеспечения безопасности web-приложений при их проектировании, разработке, внедрении, продвижении и применении в различных видах деятельности.

### Задачи дисциплины

- знакомство с основными видами веб-приложений и принципами обеспечения информационной безопасности их проектирования;
- получения навыков обеспечения информационной безопасности веб-приложений при их создании и эксплуатации..

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
ПК-2 Способен администрировать средства защиты информации в компьютерных системах и сетях	ПК-3.3ПК-2 Администрирует средства защиты информации прикладного и системного программного обеспечения	знать: - типовые механизмы защиты от кибератак на web-приложения; - требования нормативных документов регуляторов по обеспечению защиты web-приложений.  уметь: - администрировать механизмы защиты от киберугроз в системных и прикладных программных продуктах, а также web-приложениях; - разрабатывать рекомендации по применению мер защиты web-приложений при их разработке, развертыванию и использованию.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к факультативным дисциплинам основной профессиональной образовательной программе Безопасность компьютерных систем (продвинутый уровень) (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

Базируется на уровне среднего общего образования.

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

### 3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

#### 3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 часа.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания
				Контактная работа							СР			
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль	
КПР	ГК	ИККП	ТК											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Требования к безопасности web-приложений	39.7	7	10	-	8	-	-	-	-	-	21.7	-	<p><b><u>Подготовка к текущему контролю:</u></b> Повторение материала по разделу "Требования к безопасности web-приложений"</p> <p><b><u>Подготовка к аудиторным занятиям:</u></b> Проработка лекции, выполнение и подготовка к защите практических заданий</p> <p><b><u>Подготовка домашнего задания:</u></b> Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Требования к безопасности web-приложений" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам.</p> <p><b><u>Подготовка доклада, выступления:</u></b> Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: 1.</p>
1.1	Тема 1. Введение в безопасность приложений	6		2	-	1	-	-	-	-	-	3	-	
1.2	Тема 2. Жизненный цикл защиты web-приложения	6.7		2	-	1	-	-	-	-	-	3.7	-	
1.3	Тема 3. Построение программы безопасности web-приложения	9		2	-	2	-	-	-	-	-	5	-	
1.4	Тема 4. Сфера действия безопасности приложений	9		2	-	2	-	-	-	-	-	5	-	
1.5	Тема 5. Требования ГОСТ Р 56939-2016	9		2	-	2	-	-	-	-	-	5	-	

													Отличия защиты web-приложений от защиты сетей и хостов; 2. Мероприятия жизненного цикла защиты web-приложения; 3. Рекомендации по разработке внутреннего web-приложения; 4. Процесс менеджмента нормативной структуры организации; 5. Меры по разработке безопасного программного обеспечения; <b><u>Подготовка к практическим занятиям:</u></b> Изучение материала по разделу "Требования к безопасности web-приложений" подготовка к выполнению заданий на практических занятиях <b><u>Самостоятельное изучение теоретического материала:</u></b> Изучение дополнительного материала по разделу "Требования к безопасности web-приложений" <b><u>Изучение материалов литературных источников:</u></b> [1], 1-150 [2], 1-644
2	Защита Web-приложений	32	6	-	8	-	-	-	-	-	18	-	<b><u>Подготовка к текущему контролю:</u></b> Повторение материала по разделу "Защита Web-приложений"
2.1	Тема 6.. Выявление и эксплуатация SQL-инъекций в приложениях	10	2	-	2	-	-	-	-	-	6	-	<b><u>Подготовка к аудиторным занятиям:</u></b> Проработка лекции, выполнение и подготовка к защите практических заданий
2.2	Тема 7. Защита веб-приложений от атак типа XSS	10	2	-	2	-	-	-	-	-	6	-	<b><u>Подготовка домашнего задания:</u></b> Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Защита Web-приложений" материалу.
2.3	Тема 8. Применение подхода DevSecOps в современных системах разработки программного обеспечения	12	2	-	4	-	-	-	-	-	6	-	Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам.

													<p><b><u>Подготовка доклада, выступления:</u></b> Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: 1. Методы обнаружения внедрения опасных команд. OWASP; 2. Меры предотвращения DOM-based XSS. Использование CSP; 3. Сравнение некоторых SCA.</p> <p><b><u>Подготовка к практическим занятиям:</u></b> Изучение материала по разделу "Защита Web-приложений" подготовка к выполнению заданий на практических занятиях</p> <p><b><u>Самостоятельное изучение теоретического материала:</u></b> Изучение дополнительного материала по разделу "Защита Web-приложений"</p> <p><b><u>Изучение материалов литературных источников:</u></b> [1], 200-560 [3], 1-326</p>
	Зачет	0.3	-	-	-	-	-	-	-	0.3	-	-	
	Всего за семестр	72.0	16	-	16	-	-	-	-	0.3	39.7	-	
	Итого за семестр	72.0	16	-	16	-	-	-	-	0.3	39.7	-	

**Примечание:** Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПП – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

## **3.2 Краткое содержание разделов**

### 1. Требования к безопасности web-приложений

#### 1.1. Тема 1. Введение в безопасность приложений

Проблема безопасности web-приложений. Обоснование для бизнеса.. Отличия защиты web-приложений от защиты сетей и хостов.

#### 1.2. Тема 2. Жизненный цикл защиты web-приложения

Мероприятия жизненного цикла защиты web-приложения. Безопасная разработка. Безопасное развертывание. Безопасное использование.

#### 1.3. Тема 3. Построение программы безопасности web-приложения

Рекомендации по разработке программы безопасности web-приложения крупной компании. Рекомендации по разработке программы безопасности web-приложения компании среднего размера в соответствии требованиям PCI. Рекомендации по разработке внутреннего web-приложения.

#### 1.4. Тема 4. Сфера действия безопасности приложений

Требования безопасности приложений согласно ГОСТ Р ИСО/МЭК 27034-1 – 2014. Менеджмент безопасности приложений. Процесс менеджмента информационной безопасности приложений.. Нормативная структура организации (ONF).. ONF основа безопасности организации. Общая информация. Компоненты. Библиотека мер и средств контроля и управления безопасностью приложения (ASC) организации. Процесс менеджмента нормативной структуры организации.

#### 1.5. Тема 5. Требования ГОСТ Р 56939-2016

Разработка безопасного программного обеспечения. Общие требования. Меры по разработке безопасного программного обеспечения.

### 2. Защита Web-приложений

#### 2.1. Тема 6.. Выявление и эксплуатация SQL-инъекций в приложениях

Причины возникновения SQL-инъекций. Техники, применяемые при эксплуатации SQL-инъекций. Процесс обнаружения и эксплуатации SQL-инъекций. Защита веб-приложений от инъекций команд. Характеристика основ внедрения опасных команд. Методы обнаружения внедрения опасных команд. OWASP CheatSheet.

#### 2.2. Тема 7. Защита веб-приложений от атак типа XSS

Общее понятие XSS. Виды XSS. Контексты выполнения. Common Weakness Enumeration.. Меры предотвращения stored и reflected XSS. CSRF. SSRF. Меры предотвращения stored и reflected XSS. Меры предотвращения DOM-based XSS. Использование CSP.

#### 2.3. Тема 8. Применение подхода DevSecOps в современных системах разработки программного обеспечения

Понятие DevSecOps. Организация фаззинга исходного кода. Сравнение некоторых SCA.

## **3.3. Темы практических занятий**

1. Предотвращение атак, связанных с CSRF;
2. Сравнение требований по защите web-приложений с защитой сетей и хостов;
3. Требования по безопасной разработке, развертыванию и использованию web-

приложений;

4. Характеристика рекомендаций по разработке программы безопасности web-приложения;

5. Требования нормативных документов по действиям безопасного приложения;

6. Предотвращение атак, связанных с инъекциями команд;

7. Предотвращение атак, связанных с XSS;

8. Предотвращение Path/Directory Traversal и Open Redirect. Применение подхода DevSecOps в современных системах разработки программного обеспечения.

### **3.4. Темы лабораторных работ**

не предусмотрено

### **3.5 Консультации**

#### Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Требования к безопасности web-приложений"

2. Обсуждение материалов по кейсам раздела "Защита Web-приложений"

#### Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Требования к безопасности web-приложений"

2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Защита Web-приложений"

### **3.6 Тематика курсовых проектов/курсовых работ**

Курсовой проект/ работа не предусмотрены



### 3.7. Соответствие разделов дисциплины и формируемых в них компетенций

Запланированные результаты обучения по дисциплине (в соответствии с разделом 1)	Коды индикаторов	Номер раздела дисциплины (в соответствии с п.3.1)		Оценочное средство (тип и наименование)
		1	2	
<b>Знать:</b>				
требования нормативных документов регуляторов по обеспечению защиты web-приложений	ПК-3.3 <sub>ПК-2</sub>	+		Отчет/Анализ требований нормативных документов регуляторов по обеспечению защиты web-приложений
типовые механизмы защиты от кибератак на web-приложения	ПК-3.3 <sub>ПК-2</sub>	+		Отчет/Анализ типовых механизмов защиты от кибератак на web-приложения
<b>Уметь:</b>				
разрабатывать рекомендации по применению мер защиты web-приложений при их разработке, развертыванию и использованию	ПК-3.3 <sub>ПК-2</sub>	+		Домашнее задание/Формирование рекомендаций по разработке программы безопасности web-приложения кампании
администрировать механизмы защиты от киберугроз в системных и прикладных программных продуктах, а также web-приложениях	ПК-3.3 <sub>ПК-2</sub>		+	Домашнее задание/Администрирование механизмов защиты от киберугроз в системных и прикладных программных продуктах, а также web-приложениях

## **4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)**

### **4.1. Текущий контроль успеваемости**

**7 семестр**

Форма реализации: Выполнение задания

1. Администрирование механизмов защиты от киберугроз в системных и прикладных программных продуктах, а также web-приложениях (Домашнее задание)
2. Анализ типовых механизмов защиты от кибератак на web-приложения (Отчет)
3. Анализ требований нормативных документов регуляторов по обеспечению защиты web-приложений (Отчет)
4. Формирование рекомендаций по разработке программы безопасности web-приложения кампании (Домашнее задание)

Балльно-рейтинговая структура дисциплины является приложением А.

### **4.2 Промежуточная аттестация по дисциплине**

Зачет (Семестр №7)

В диплом выставляется оценка за 7 семестр.

**Примечание:** Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

## **5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

### **5.1 Печатные и электронные издания:**

1. Кибербезопасность цифровой индустрии : теория и практика функциональной устойчивости к кибератакам / Д. П. Зегжда, Е. Б. Александрова, М. О. Калинин, [и др.] ; ред. Д. П. Зегжда . – Москва : Горячая Линия-Телеком, 2020 . – 560 с. - Авторы указаны на обороте тит. л. - ISBN 978-5-9912-0827-7 .;
2. Белоус, А. И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения / А. И. Белоус . – Москва; Вологда : Инфра-Инженерия, 2020 . – 644 с. - ISBN 978-5-9729-0512-6 .;
3. Диогенес Ю., Озкайя Э.- "Кибербезопасность. стратегия атак и обороны", Издательство: "ДМК Пресс", Москва, 2020 - (326 с.)  
<https://e.lanbook.com/book/131717>.

### **5.2 Лицензионное и свободно распространяемое программное обеспечение:**

1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;
4. Видеоконференции (Майнд, Сберджаз, ВК и др);
5. Windows Server / Серверная операционная система семейства Linux;
6. Kali Linux.

### 5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:

1. ЭБС Лань - <https://e.lanbook.com/>
2. ЭБС "Университетская библиотека онлайн" - [http://biblioclub.ru/index.php?page=main\\_ub\\_red](http://biblioclub.ru/index.php?page=main_ub_red)
3. Научная электронная библиотека - <https://elibrary.ru/>
4. База данных Web of Science - <http://webofscience.com/>
5. База данных Scopus - <http://www.scopus.com>
6. ЭБС "Консультант студента" - <http://www.studentlibrary.ru/>
7. Журнал Science - <https://www.sciencemag.org/>
8. Электронная библиотека МЭИ (ЭБ МЭИ) - <http://elib.mpei.ru/login.php>
9. Информационно-справочная система «Кодекс/Техэксперт» - <Http://proinfosoft.ru;>  
<http://docs.cntd.ru/>
10. Национальный портал онлайн обучения «Открытое образование» - <https://openedu.ru>
11. Федеральный портал "Российское образование" - <http://www.edu.ru>

### 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	М-510, Учебная лаборатория информационно-аналитический технологий - компьютерный класс	стул, стол письменный, мультимедийный проектор, экран, доска маркерная, компьютер персональный, кондиционер
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения практических занятий, КР и КП	М-511, Учебная аудитория	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
	М-510, Учебная лаборатория информационно-аналитический технологий - компьютерный класс	стул, стол письменный, мультимедийный проектор, экран, доска маркерная, компьютер персональный, кондиционер
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Учебные аудитории для проведения промежуточной аттестации	М-510, Учебная лаборатория информационно-аналитический технологий - компьютерный класс	стул, стол письменный, мультимедийный проектор, экран, доска маркерная, компьютер персональный, кондиционер
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Помещения для самостоятельной работы	НТБ-201, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный,

		принтер, кондиционер
	К-307, Учебная лаборатория "Открытое программное обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
	К-302, Учебная лаборатория "Информационно-аналитические технологии"	стол преподавателя, стол компьютерный, стул, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
Помещения для консультирования	М-510, Учебная лаборатория информационно-аналитический технологий - компьютерный класс	стул, стол письменный, мультимедийный проектор, экран, доска маркерная, компьютер персональный, кондиционер
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

## БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

### Безопасность Web-приложений

(название дисциплины)

#### 7 семестр

**Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:**

- КМ-1 Анализ типовых механизмов защиты от кибератак на web-приложения (Отчет)
- КМ-2 Формирование рекомендаций по разработке программы безопасности web-приложения кампании (Домашнее задание)
- КМ-3 Анализ требований нормативных документов регуляторов по обеспечению защиты web-приложений (Отчет)
- КМ-4 Администрирование механизмов защиты от киберугроз в системных и прикладных программных продуктах, а также web-приложениях (Домашнее задание)

**Вид промежуточной аттестации – Зачет.**

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Требования к безопасности web-приложений					
1.1	Тема 1. Введение в безопасность приложений		+			
1.2	Тема 2. Жизненный цикл защиты web-приложения		+			
1.3	Тема 3. Построение программы безопасности web-приложения			+		
1.4	Тема 4. Сфера действия безопасности приложений				+	
1.5	Тема 5. Требования ГОСТ Р 56939-2016				+	
2	Защита Web-приложений					
2.1	Тема 6.. Выявление и эксплуатация SQL-инъекций в приложениях					+
2.2	Тема 7. Защита веб-приложений от атак типа XSS					+
2.3	Тема 8. Применение подхода DevSecOps в современных системах разработки программного обеспечения					+
Вес КМ, %:			15	35	15	35