

Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Алтайский государственный технический университет им. И.И. Ползунова»

**СОГЛАСОВАНО**

Декан ФИТ  
Авдеев

А.С.

## **Рабочая программа дисциплины**

**Код и наименование дисциплины: Б1.В.6 «Технологии защиты веб-ресурсов»**

**Код и наименование направления подготовки (специальности): 10.03.01  
Информационная безопасность**

**Направленность (профиль, специализация): Организация и технологии  
защиты информации (в сфере техники и технологий, связанных с  
обеспечением защищенности объектов информатизации)**

**Статус дисциплины: часть, формируемая участниками образовательных  
отношений**

**Форма обучения: очная**

<b>Статус</b>	<b>Должность</b>	<b>И.О. Фамилия</b>
Разработал	старший преподаватель	П.А. Теплюк
Согласовал	Зав. кафедрой «ИВТиБ»	А.Г. Якунин
	руководитель направленности (профиля) программы	Е.В. Шарлаев

г. Барнаул

**1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций**

Компетенция	Содержание компетенции	Индикатор	Содержание индикатора
ПК-3	Способен применять технологии защиты информации в сфере профессиональной деятельности	ПК-3.2	Способен организовывать защиту данных в информационных системах

**2. Место дисциплины в структуре образовательной программы**

Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	Информатика, Информационные технологии, Организация и технологии защиты данных в информационных системах, Программирование, Технологии и методы программирования
Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	Комплексная защита объектов информатизации, Преддипломная практика, Технологии защиты информации в вычислительных сетях

**3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающегося с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающегося**

Общий объем дисциплины в з.е. /час: 4 / 144

Форма промежуточной аттестации: Зачет

Форма обучения	Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
	Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
очная	32	0	32	80	76

**4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий**

**Форма обучения: очная**

**Семестр: 7**

**Лекционные занятия (32ч.)**

**1. Общее представление об организации защиты данных в веб-ресурсах {беседа} (4ч.) [1,3,10,12] Технологии получения и безопасной передачи информации в сети Интернет. Основные принципы организации защиты**

данных в веб-ресурсах. Принципы безопасного использования веб-ресурсов. Понятие безопасности приложений и классификация опасностей. Источники угроз информационной безопасности и меры по их предотвращению. Регламенты и методы разработки безопасных веб-приложений

2. Современные угрозы безопасности веб-ресурсов {беседа} (10ч.)[1,3,4,6,12] Классификация современных угроз безопасности веб-ресурсов OWASP Top 10. Уязвимости, связанные с внедрением команд и кода: SQL, NoSQL, OS, LDAP. Недостатки механизмов аутентификации. Уязвимости, ведущие к разглашению конфиденциальной информации. Внедрение внешних XML-сущностей. Недостатки контроля доступа. Некорректная настройка параметров безопасности. Межсайтовое выполнение сценариев. небезопасная десериализация. Использование компонентов с известными уязвимостями. Недостатки журналирования и мониторинга

3. Аудит безопасности и организация защиты данных в веб-ресурсах {беседа} (10ч.)[1,3,4,6,7,9,10,11,12,13,15,16] Роль аудита безопасности веб-ресурсов при организации защиты данных в информационных системах. Тестирование на проникновение как важный элемент аудита безопасности веб-ресурса. Методы "черного", "серого" и "белого" ящика при тестировании на проникновение. Этапы проведения тестирования на проникновение. DNS-разведка. Сбор информации из открытых источников (OSINT). Сбор информации о сервере. Сканирование контента. Фаззинг входных параметров. Поиск утечек данных. Тестирование аутентификации. Отслеживание и перехват сессий. Атака с внедрением команд ОС. Включение файлов и обход каталогов. SQL-инъекции. XXE. Межсайтовое выполнение сценариев. Межсайтовая подделка запроса. Атаки на логические уязвимости веб-ресурсов. Методы и средства организации защиты данных в веб-ресурсах.

4. Методы и средства безопасной разработки веб-ресурсов {беседа} (8ч.)[1,2,5,10] Обзор рекомендаций OWASP по безопасной разработке веб-ресурсов. Безопасное взаимодействие и работа с данными из БД. Использование безопасных сторонних библиотек и фреймворков. Использование безопасных алгоритмов аутентификации. Организация защиты от DDoS-атак. Шифрование веб-трафика с использованием SSL. Проверка корректности пользовательских данных на клиенте и сервере. Безопасная конфигурация инфраструктуры веб-ресурса.

#### **Практические занятия (32ч.)**

1. Сбор данных о веб-ресурсе из открытых источников {творческое задание} (6ч.)[1,2,3,6,7,8] Цель работы: получение практических навыков поиска и анализа исходных данных веб-ресурса на основе открытых источников

2. Выявление уязвимостей в веб-ресурсе методом активного сканирования {творческое задание} (6ч.)[1,2,6,7,8,9,15,16] Цель работы: получение практических навыков работы со сканерами безопасности, позволяющими

выявлять в веб-ресурсе известные уязвимости

3. Организация защиты веб-ресурса от внедрения кода {творческое задание} (8ч.)[1,2,4,6,7,8,11,13,16] Цель работы: получение практических навыков проведения SQL- и других типов инъекций и организации защиты веб-ресурса от них

4. Организация защиты веб-ресурса от атак XSS и XXE {творческое задание} (8ч.)[1,3,6,7,8,11,16] Цель работы: получение практических навыков проведения атаки XSS и XXE различных типов и организации защиты веб-ресурса от них

5. Организация безопасной разработки веб-ресурса {творческое задание} (4ч.)[1,2,5,7,8,10,12,14] Цель работы: получение практических навыков безопасной разработки и развертывания веб-ресурса

#### Самостоятельная работа (80ч.)

1. Подготовка к лекциям и практическим занятиям {с элементами электронного обучения и дистанционных образовательных технологий} (16ч.)[1,3,4,6,7,8,9,10,11,12,13,14,15,16]

2. Выполнение расчётного задания(28ч.)[1,3,4,6,7,8,9,11,12,13,15,16] Тематика расчетного задания: аудит безопасности тестового веб-ресурса методом "черного" ящика

3. Подготовка к зачету(36ч.)[1,2,3,4,5,6,7,12]

5. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Для каждого обучающегося обеспечен индивидуальный неограниченный доступ к электронной информационно-образовательной среде АлтГТУ:

1. Якунин А.Г. Учебно-методическое пособие по дисциплине «Основы WEB-технологий».- Барнаул, АлтГТУ, 2011. 173 с. Источник: электронная библиотека образовательных ресурсов АлтГТУ. Режим доступа: <http://elib.altstu.ru/eum/download/vsib/WEB-Jakunin.pdf>

2. Теплюк П.А. Методические рекомендации к выполнению лабораторных работ по дисциплине «Безопасность WEB-технологий». - Барнаул, АлтГТУ, 2023. 30 с. Источник: электронная библиотека образовательных ресурсов АлтГТУ. Режим доступа: <http://elib.altstu.ru/eum/download/ivtib/uploads/teplyuk-p-a-ivtib-63ce11ab3846d.pdf>

6. Перечень учебной литературы

## 6.1. Основная литература

1. Защита Web-приложений : учебное пособие : [16+] / А. В. Скрыпников, Д. В. Арапов, В. В. Денисенко, Т. Д. Герасимова ; науч. ред. И. А. Хаустов ; Воронежский государственный университет инженерных технологий. – Воронеж : Воронежский государственный университет инженерных технологий, 2020. – 77 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=612405> (дата обращения: 21.03.2023). – Библиогр. в кн. – ISBN 978-5-00032-469-1. – Текст : электронный.

2. Марухленко, А. Л. Разработка защищённых интерфейсов Web-приложений : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов. – Москва ; Берлин : Директ-Медиа, 2021. – 175 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=599050> (дата обращения: 21.03.2023). – Библиогр. в кн. – ISBN 978-5-4499-1676-1. – DOI 10.23681/599050. – Текст : электронный.

3. Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=598988> (дата обращения: 21.03.2023). – Библиогр.: с. 196-205. – ISBN 978-5-4499-1671-6. – DOI 10.23681/598988. – Текст : электронный.

## 6.2. Дополнительная литература

4. Брюхомицкий, Ю. А. Безопасность информационных технологий : учебное пособие : в 2 частях : [16+] / Ю. А. Брюхомицкий ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2020. – Часть 1. – 171 с. : ил., табл., схем., граф. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=612167> (дата обращения: 21.03.2023). – Библиогр. в кн. – ISBN 978-5-9275-3571-2 (Ч. 1). – ISBN 978-5-9275-3526-2. – Текст : электронный.

5. Вагин, Д. В. Современные технологии разработки веб-приложений : учебное пособие : [16+] / Д. В. Вагин, Р. В. Петров ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 52 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=573960> (дата обращения: 21.03.2023). – ISBN 978-5-7782-3939-5. – Текст : электронный.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

6. OWASP Top 10 Web Application Security Risks <https://owasp.org/www-project-top-ten/>
7. OWASP Web Security Testing Guide <https://owasp.org/www-project-web-security-testing-guide/>
8. Oracle VirtualBox <https://www.virtualbox.org/>
9. OWASP ZAP <https://owasp.org/www-project-zap/>
10. Журнал "Хакер" <https://xakep.ru/>
11. BurpSuite <https://portswigger.net/burp>
12. Web Security Academy <https://portswigger.net/web-security>
13. Sqlmap <https://github.com/sqlmapproject/sqlmap>
14. Центр Сертификации Let's Encrypt <https://letsencrypt.org/ru/>
15. OpenVAS <https://www.openvas.org/>
16. Metasploit Framework <https://www.metasploit.com/>
17. Root Me: hacking and information security learning platform <https://www.root-me.org/>

#### **8. Фонд оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации**

Содержание промежуточной аттестации раскрывается в комплекте контролирующих материалов, предназначенных для проверки соответствия уровня подготовки по дисциплине требованиям ФГОС, которые хранятся на кафедре-разработчике РПД в печатном виде и в ЭИОС.

#### **9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем**

Для успешного освоения дисциплины используются ресурсы электронной информационно-образовательной среды, образовательные интернет-порталы, глобальная компьютерная сеть Интернет. В процессе изучения дисциплины происходит интерактивное взаимодействие обучающегося с преподавателем через личный кабинет студента.

<b>№пп</b>	<b>Используемое программное обеспечение</b>
1	LibreOffice
1	CentOS Linux
2	Chrome
2	Windows
3	Антивирус Kaspersky
4	Linux
5	Mozilla Firefox
6	Python
7	VirtualBox
9	Wireshark

<b>№пп</b>	<b>Используемые профессиональные базы данных и информационные</b>
------------	---

<b>справочные системы</b>	
1	Национальная электронная библиотека (НЭБ) – свободный доступ читателей к фондам российских библиотек. Содержит коллекции оцифрованных документов (как открытого доступа, так и ограниченных авторским правом), а также каталог изданий, хранящихся в библиотеках России. ( <a href="http://нэб.рф/">http://нэб.рф/</a> )

#### **10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

<b>Наименование специальных помещений и помещений для самостоятельной работы</b>
учебные аудитории для проведения учебных занятий
помещения для самостоятельной работы

Материально-техническое обеспечение и организация образовательного процесса по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья осуществляется в соответствии с «Положением об обучении инвалидов и лиц с ограниченными возможностями здоровья».