Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УТВЕРЖДАЮ
Проректор по учебной работе
_____ В.А. Прытков
31.03.2020 г.

Регистрационный № УД-6-1409/уч.

«ЗАЩИТА ВЕБ-РЕСУРСОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА»

Учебная программа учреждения высшего образования по учебной дисциплине
для специальности:
1-98 80 01 «Информационная безопасность»

2020 г.

Учебная программа учреждения высшего образования составлена на основе образовательного стандарта ОСВО 1-98 80 01-2019 и учебных планов специальности 1-98 80 01 «Информационная безопасность».

Составитель:
Е.С. Белоусова, доцент кафедры защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат технических наук.

Рецензенты:
Кафедра телекоммуникационных систем учреждения образования «Белорусская государственная академия связи» (протокол № 8 от 25.02.2020г.);
В.Ю. Цветков, заведующий кафедрой инфокоммуникационных технологий учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», доктор технических наук, профессор.

Рассмотрена и рекомендована к утверждению:
Кафедрой защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № 11 от 06.03.2020г.);
Научно-методическим советом учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № 7 от 20.03.2020г.).

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа рассчитана на 198 учебных часов (6 з.е.)

План учебной дисциплины в дневной форме обучения:

Код специальности	Название специальности	Курс	Семестр	Аудиторных часов (в соответствии с учебным планом УВО)				Форма текущей аттестации
				Всего	Лекции	Лабораторные занятия	Практические занятия, семинары	
1-98 80 01	Информационная безопасность	2	3	62	38	24	–	Экзамен

План учебной дисциплины в заочной форме обучения:

Код специальности	Название специальности	Курс	Семестр	Аудиторных часов (в соответствии с учебным планом УВО)				Контрольная работа	Форма текущей аттестации
				Всего	Лекции	Лабораторные занятия	Практические занятия, семинары		
1-98 80 01	Информационная безопасность	2	3	16	8	8	–	1	Экзамен

Место учебной дисциплины.

Учебная дисциплина «Защита веб-ресурсов от несанкционированного доступа» является неотъемлемой составной частью подготовки магистров по специальности 1-98 80 01 «Информационная безопасность» и относится числу дисциплин модуля «Безопасность веб-технологий».

За последние время число официально зарегистрированных компьютерных преступлений возросло в несколько раз. При этом механизмы атак постоянно совершенствуются, поэтому требуется поиск все новых путей устранения угроз. Весьма актуальным является подготовка специалистов, владеющих методами поиска и устранения уязвимостей в разрабатываемых веб-приложениях. Для успешного усвоения учебной дисциплины «Защита веб-ресурсов от несанкционированного доступа» необходимы базовые и специальные знания, полученные при осво-

ении содержания образовательных программ по специальностям I ступени высшего образования. Дисциплина «Защита веб-ресурсов от несанкционированного доступа» тесно взаимосвязана со следующими дисциплинами: «Безопасность баз данных», «Организация данных в сетевых приложениях», «Виртуализация в информационных системах».

Цель учебной дисциплины: приобретение знаний об основных понятиях безопасности веб-технологий, ознакомление с технологиями защиты веб-приложений, формирование навыков проведения анализа защищённости веб-приложений и конфигурирования средств защиты от веб-атак.

Задачи учебной дисциплины:

– формирование базовых представлений о структуре построения веб-приложений;

– овладение различными методами анализа и обнаружения уязвимостей в веб-приложениях;

– приобретение навыков противодействия веб-атакам;

– развитие навыков анализа и прогнозирования инцидентов информационной безопасности.

В результате изучения учебной дисциплины «Защита веб-ресурсов от несанкционированного доступа» формируются следующие компетенции:

специализированные:

– проводить анализ защиты веб-ресурсов и обоснованно выбирать и настраивать средства защиты информации.

В результате изучения учебной дисциплины магистрант должен:

знать:

– принципы установления соединения клиента с сервером;

– методы поиска уязвимостей в веб-приложениях;

– принципы построения эффективных систем аутентификации и разграничения доступа к веб-ресурсам;

– основные уязвимости и атаки на веб-приложения;

уметь:

– выявлять уязвимости с использованием различных средств анализа защищенности;

– настраивать системы безопасности компонентов веб-приложения (операционной системы, систем управления базами данных и др.);

– конфигурировать специализированные средства защиты веб-приложений, такие как Web Application Firewall (WAF);

владеть:

– современными методами тестирования веб-приложений на наличие уязвимостей;

– приемами администрирования Web Application Firewall (WAF) для защиты веб-приложений от внешних угроз.

Перечень учебных дисциплин, усвоение которых необходимо для изучения данной учебной дисциплины.

№ п.п.	Название учебной дисциплины	Раздел, темы
1	Базируется на знаниях, полученных при освоении содержания образовательных программ по специальностям I ступени высшего образования	

1. Содержание учебной дисциплины

№ тем	Наименование разделов, тем	Содержание тем
1	Основные понятия веб-технологий	Понятия «клиент», «сервер», «приложение». Область применения веб-приложений. Уровни информационной инфраструктуры. Структура веб-приложения. Виды серверов. HTTP-сервер. Отличия Apache и Nginx. Языки программирования для создания веб-приложений.
2	Базовые сведения о веб-технологиях	Методы передачи данных. Механизмы обмена данных между клиентом и сервером. HTTP протокол передачи данных. Структура запросов и ответов сервера.
3	Безопасная конфигурация сервера	Операционные системы для серверов. Сравнение ОС Linux и Windows. Структура файловой системы Linux. Категории пользователей. Доступ к серверу ОС Linux
4	Базы данных	Базы данных. Системы управления базами данных. Взаимодействие клиента с базами данных. Построение запросов к базам данных.
5	Тестирование на проникновение	Сбор злоумышленником информации о настройках сервера. Методология анализа защищенности. Автоматизированные средства поиска уязвимостей.
6	Безопасность установления соединения	Протоколы SSL и TLS. Уязвимости ранних версий протоколов. Механизмы реализации атаки SSL и методы противодействия.
7	Уязвимости и атаки на веб-приложения	Основные источники уязвимостей. Методы оценки уязвимостей системы. Источники информации об уязвимостях. Причины возникновения уязвимостей. Атаки на веб-приложения. Список OWASP TOP 10. Классификация угроз Web Application Security Consortium.
8	Инъекции вредоносного кода	Механизмы реализации атак SQL Injection, OS Command Injection. Виды атак SQL Injection.
9	Уязвимости XML-объектов	Формат HTML и XML-документов (DOM, DTD). Форматы определения правил валидности XML-документов. Уязвимости HTML-документов
10	Межсайтовое выполнение сценариев	Атака XSS и механизм ее реализации. Подмена содержимого веб-ресурса. Варианты атак. Отраженный вариант атаки. Использование внедрения сценариев. Защита от внедрения сценариев. Подделка HTTP-запросов
11	Механизмы управления сессией	Уязвимые механизмы аутентификации и управления сессией. Тестирование защищенности механизма управления доступом и сессий
12	Межсетевые экраны для веб-приложений	Общая классификация способов противодействия атакам. Межсетевые экраны для веб-приложений (Web Application Firewalls). Блокирование атак средствами Web Application Firewall. Возможности и ограничения WAF. Примеры реализации WAF.
13	Небезопасная десериализация	Отличие десериализации и сериализации. Уязвимости передаваемых типов данных.
14	Использование компонентов с известными уязвимостями	Варианты эксплуатации уязвимостей веб-сервиров. Обнаружение атак средствами контроля целостности файлов. Сигнатурное блокирование атак. Уменьшение поверхности атаки за счет уточнения конфигурации веб-сервера.
15	Недостаточное	Проблемы мониторинга событий. Недостаточные средства сбора со-

№ тем	Наименование разделов, тем	Содержание тем
	журналирование и мониторинг	общений о событиях. Администрирование привилегий. Реагирование на инциденты. Типовая структура SIEM-систем.

2. Информационно-методический раздел

2.1 Литература

2.1.1 Основная

1. Сердюк В. А. Новое в защите от взлома корпоративных систем : учебник / В. А. Сердюк. – М. : Техносфера, 2007. – 360 с. – (Мир программирования).

2. Информационная безопасность открытых систем : учебник для студентов вузов [доп. МО РФ]. Т. 2 : Средства защиты в сетях / С. В. Запечников [и др.]. – М. : Горячая линия-Телеком, 2008. – 558 с.

3. OWASP Top 10 Most Critical Web Application Security Risks [Электронный ресурс] : Document for web application security / The Open Web Application Security Project (OWASP). – Режим доступа : https://www.owasp.org/images/7/72 /OWASP_Top_10-2017_%28en%29.pdf.pdf

2.1.2 Дополнительная

1. Гафнер, В. В. Информационная безопасность : учебное пособие / В. В. Гафнер. – Ростов н/Д. : Феникс, 2010. – 324 с. – (Высшее образование).

2. Защита информации : учебное пособие / А. П. Жук [и др.]. – М. : РИОР : ИНФРА-М, 2013. – 392 с. – (Высшее образование).

3. Пулко, Т. А. Введение в информационную безопасность : учебное пособие / Т. А. Пулко. – Минск : БГУИР, 2018. – 164 с. : ил.

2.2 Перечень компьютерных программ, наглядных и других пособий, методических указаний и материалов, технических средств обучения, оборудования для выполнения лабораторных работ

1. Программный продукт виртуализации Oracle VM VirtualBox.
2. Виртуальный диск с операционной системой Kali Linux.
3. Виртуальный диск с операционной системой веб-сервера с приложением WebGoat.
4. Виртуальный диск с операционной системой Web Application Firewall.

2.3. Перечень тем лабораторных занятий, их название

Основная цель проведения лабораторных занятий состоит в закреплении теоретического материала курса, приобретении навыков выполнения эксперимента, обработки экспериментальных данных, анализа результатов, грамотного оформления отчетов.

№ темы по п.1	Наименование лабораторной работы	Содержание	Обеспеченность по пункту 2.2
2	Соединение клиента с веб-приложением	Изучение процесса взаимодействия пользователя с веб-ресурсом по протоколу HTTP	1–3
3	Удаленное управление сервером	Овладение методами и средствами сбора информации об анализируемом веб-приложении.	1–3
4	Сбор информации о защищенности веб-сервера	Овладение методами и средствами сбора информации об анализируемом веб-приложении	1–3
6	Тестирование защищенности механизма управления доступом и сессий	Овладение методами тестирования защищенности механизма управления доступом и сессий	1–3
6	Основы безопасности веб-ресурса	Установка и настройка Web Application Firewalls	1–4
8	Поиск уязвимостей к атакам SQL-injection	Изучение базовых конструкций SQL-запросов и овладение навыками их использования для атаки SQL-injection	1–3
10	Межсайтовый скриптинг	Изучение механизмов реализации атак межсайтового скпринтинга, овладение методами тестирования веб-ресурсов на внедрение произвольного кода в HTML-страницу	1–3
11	Безопасность SSL и TLS соединений и контроля доступа	Web Application Firewall для противодействия атаке SSL Strip. Противодействие атакам обхода механизмов контроля доступа	1–4
12	Блокирование перехвата пользовательских данных	Направление запросов для инспекции в WAF. Механизмы обработки запросов в WAF	1–4
12	Блокирование атак SQL Injection	Настройки политик безопасности Web Application Firewall для блокирования атак OS Command Injection, SQL Injection	1–4
12	Организация безопасности критичных данных	Противодействие раскрытию критичных данных средствами Web Application Firewall	1–4
12	Защита запросов к веб-ресурсу	Сигнатурное блокирование XSS средствами Web Application Firewall	1–4

2.4. Контрольная работа

Целью контрольной работы является углубление знаний, приобретение исследовательских навыков. Контрольная работа выполняется магистрантами заочной формы обучения на основе индивидуальных заданий. Вариант индивидуального задания контрольной работы выдается магистранту преподавателем.

№ темы по п.1	Наименование контрольной работы	Содержание	Обеспеченность по пункту 2.2
10	Тестирование веб-приложения	Поиск и анализ уязвимостей веб-приложения, оценка уровня защищенности	1–4

2.5 Перечень рекомендуемых средств диагностики результатов учебной деятельности

Для диагностики результатов учебной деятельности могут использоваться следующие формы:

1. Защита лабораторной работы.
2. Устный опрос
3. Защита контрольной работы.
4. Коллоквиум

3.1 Учебно-методическая карта учебной дисциплины в дневной форме обучения

Номер раздела, темы по	Название раздела, темы	Количество аудиторных часов			Самостоятельная работа, часы	Форма контроля знаний
		ЛК	Лаб. зан.	ПЗ		
1	Основные понятия веб-технологий	2	-	-	10	Устный опрос
2	Базовые сведения о веб-технологиях	2	2	-	9	Устный опрос, защита лабораторной работы
3	Безопасная конфигурация сервера	4	2	-	9	Устный опрос, защита лабораторной работы
4	Базы данных	2	2	-	9	Устный опрос, защита лабораторной работы
5	Тестирование на проникновение	2	-	-	9	Устный опрос
6	Безопасность установления соединения	2	4	-	9	Устный опрос, защита лабораторной работы
7	Уязвимости и атаки на веб-приложения	2	-	-	9	Устный опрос
8	Инъекции вредоносного кода	4	2	-	9	Устный опрос, защита лабораторной работы
9	Уязвимости XML-объектов	2	-	-	9	Устный опрос
10	Межсайтовое выполнение сценариев	4	2	-	9	Устный опрос, защита лабораторной работы
11	Механизмы управления сессией	2	2	-	9	Устный опрос, защита лабораторной работы
12	Межсетевые экраны для веб-приложений	4	8	-	9	Устный опрос, защита лабораторной работы
13	Небезопасная десериализация	2	-	-	9	Устный опрос
14	Использование компонентов с известными уязвимостями	2	-	-	9	Устный опрос
15	Недостаточное журналирование и мониторинг	2	-	-	9	Устный опрос
	Текущая аттестация					**Экзамен**
	Итого	**38**	**24**	**-**	**136**	

3.1 Учебно-методическая карта учебной дисциплины в заочной форме обучения

Номер раздела, темы по п.1	Название раздела, темы	Количество аудиторных часов			Самостоятельная работа, часы	Форма контроля знаний
		ЛК	Лаб. зан.	ПЗ		
1	Основные понятия веб-технологий	-	-	-	12	Коллоквиум
2	Базовые сведения о веб-технологиях	-	-	-	14	Коллоквиум
3	Безопасная конфигурация сервера	2	2	-	12	Защита лабораторной работы
4	Базы данных	-	-	-	12	Коллоквиум
5	Тестирование на проникновение	-	-	-	12	Коллоквиум
6	Безопасность установления соединения	-	2	-	12	Коллоквиум
7	Уязвимости и атаки на веб-приложения	2	-	-	12	Защита лабораторной работы
8	Инъекции вредоносного кода	2	2	-	12	Защита лабораторной работы
9	Уязвимости XML-объектов	-	-	-	12	Коллоквиум
10	Межсайтовое выполнение сценариев	-	-	-	12	Коллоквиум, защита контрольной работы
11	Механизмы управления сессией	-	-	-	12	Коллоквиум
12	Межсетевые экраны для веб-приложений	2	2	-	12	Защита лабораторной работы
13	Небезопасная десериализация	-	-	-	12	Коллоквиум
14	Использование компонентов с известными уязвимостями	-	-	-	12	Коллоквиум
15	Недостаточное журналирование и мониторинг	-	-	-	12	Коллоквиум
	Текущая аттестация					**Экзамен**
	Итого	**8**	**8**	**-**	**182**	

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ С ДРУГИМИ УЧЕБНЫМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Код и наименование специальности	Выпускающая кафедра	Предложения об изменениях в содержании по изучаемой учебной дисциплине	Подпись заведующего выпускающей кафедрой с указанием номера протокола и даты заседания кафедры
1	2	3	4
1-98 80 01 «Информационная безопасность»	Защиты информации	Нет	_____ Т.В. Борботько Протокол № 11 от 06.03.2020г.

Заведующий кафедрой защиты информации _____Т.В. Борботько