МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
заведующий кафедрой
кибербезопасности
информационных систем
С.Л. Кенин

22.03.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.ДВ.03.01 Безопасность интернет-приложений

1. Шифр и наименование направления подготовки/специальности:
10.05.01 Компьютерная безопасность

2. Профиль подготовки / специализация / магистерская программа:
Математические методы защиты информации

3. Квалификация (степень) выпускника:
Специалист

4. Форма обучения:
Очная

5. Кафедра, отвечающая за реализацию дисциплины:
кафедра кибербезопасности информационных систем

6. Составители программы:
Ляликова Виктория Геннадиевна,
кандидат физико-математических наук, доцент

7. Рекомендована:
научно-методическим советом факультета ПММ, протокол №7 от 22.03.2024 г.

_____

(отметки о продлении вносятся вручную)

8. Учебный год: 2027/2028 **Семестр(-ы):** 8

9. **Цели и задачи учебной дисциплины**

Цели изучения дисциплины: получение знаний о принципах построения архитектуры ИР, особенностях аппаратного и программного обеспечения ИР; формирование знаний об основных типах атак на web-приложения и методах их предотвращения; приобретение опыта анализа научно-технической информации и результатов исследований.

Задачи изучения дисциплины:

− изучение принципов построения архитектуры ИР, особенностей аппаратного и программного обеспечения ИР;

– изучение подходов и отдельных методик проведения экспертной оценки функционирования информационных ресурсов и планирование методов их реализации;

- изучение основных типов атак на web-приложения и методах их предотвращения; - приобретение опыта организации и руководства проектированием, проверкой работоспособности информационных ресурсов, проведения экспертной оценки функционирования ИР;

- получение навыков рационального выбора и настройки аппаратно-программных элементов web-приложения.

10. Место учебной дисциплины в структуре ОПОП: дисциплина относится к части, формируемой участниками образовательных отношений, блока Б1 дисциплин учебного плана.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения

Код	Название компетенции	Код(ы)	Индикаторы(ы)	Планируемые результаты обучения
ПК-2	Способен проводить исследования на всех этапах жизненного цикла средств защиты информации в профессиональной деятельности	ПК-2.1	Применяет эффективные методы и средства планирования и организации исследований и разработок.	Знать: способы проведения оценки средств защиты информации в профессиональной деятельности; уметь: применять эффективные методы и средства планирования и организации разработок; владеть (иметь навык(и)): эффективными методами средств защиты информации в профессиональной деятельности и средствами планирования и организации исследований..

ПК-3 олш1й	Способен осуществлять разработку, анализ и обосновывать эффективность применяемых математических методов защиты информации, возникающих при работе программных и программно-аппаратных средств защиты информации при решении профессиональных, исследовательских и прикладных задач	ПК-3.1	Формирует и применяет аналитическую модель эффективности внедрения средств защиты информации различных классов.	Знать: эффективность математических методов защиты информации, возникающих при работе программных средств защиты информации уметь: применять аналитические модели эффективности внедрения средств защиты информации различных классов; владеть (иметь навык(и)): навыками эффективного внедрения средств защиты информации различных классов в программные алгоритмы
		ПК-3.4	Разрабатывает программные алгоритмы, реализующие современные математические методы защиты информации	

12. Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом —3/108.

Форма промежуточной аттестации зачет.

12. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость (часы)
Аудиторные занятия		56
в том числе:	лекции	28
	практические	-
	лабораторные	28
Самостоятельная работа		88
Контроль		-
Итого:		144
Форма промежуточной аттестации		Зачет

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1. Лекции		
1.1	Основы Интернет безопасности	Веб-серверы и браузеры. Защита клиентских рабочих станций от атак Интернет. Вредоносное программное обеспечение. Критические уязвимости операционной системы. Эскалация привилегий. Социальная инженерия. Безопасность банковских операций. Антивирусное ПО. Безопасные расширения браузеров (NoScript). Двухфакторная аутентификация и ее уязвимости. Фишинг. Межсайтовый скриптинг. SQL-иньекция. Фальсификация MAC, IP и доменных адресов. Технологии Proxy и VPN. Установка и настройка WEB-сервера IIS. Аутентификация WEB. Интегрированная аутентификация. Паспорт-аутентификация. Безопасность виртуальных каталогов. Защита сайта от Google индексирования. Настройка брандмауэра.
2.	Разработка ASP.NET MVC приложений	Технологии разработки активных WEB-страниц. Язык HTML. WEB-формы. Протокол HTTP и HTTPS. Спецификация CGI. Структура ASP.NET MVC приложения. Модели, контроллеры, действия, представления. Персонализация сайта. Cookies. Сеансовые переменные и профили. Применение профилей пользователей на примере систем электронной коммерции. Безопасное хранение паролей и строк соединения с базой данных.
1.2	Различные виды атак на web-приложения	Атаки грубая сила, отказ в обслуживании, межсайтинговый скриптинг, SQL – инъекции, XML-инъекции. Примеры. Способы защиты.
2. Лабораторные работы		
2.1	Атака «межсайтовый скриптинг»	Примеры по теме «Атака «межсайтовый скриптинг»» и их разбор. Выполнение задания лабораторной работы.
2.2	Атака «снятие отпечатков пальцев»: методы и утилиты.	Примеры по теме «Атака «снятие отпечатков пальцев»: методы и утилиты» и их разбор. Выполнение задания лабораторной работы.
2.3	Атака «инъекция команд в протоколы электронной почты»	Примеры по теме «Атака «инъекция команд в протоколы электронной почты»» и их разбор. Выполнение задания лабораторной работы.
2.4	Атака «навигация по	

	запрещенным путям» Атаки «SQLинъекция» и «XMLинъекция»	Примеры теме «Атака «навигация по запрещенным путям» Атаки «SQL-инъекция» и «XML-инъекция»» и их разбор. Выполнение задания лабораторной работы.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Основы Интернет безопасности	8			18	26
2	Разработка ASP.NET MVC приложений	12		10	40	62
3	Различные виды атак на web-приложения	8		18	30	56
	Итого:	28		28	88	144

14. Методические указания для обучающихся по освоению дисциплины Освоение дисциплины включает в себя лекционные занятия, лабораторные работы и самостоятельную работу обучающихся. На первом занятии студент получает информацию для доступа к комплексу учебно-методических материалов.

Лекционные занятия посвящены рассмотрению теоретических основ. Лабораторные работы предназначены для формирования умений и навыков, закрепленных компетенций по ОПОП. Самостоятельная работа студентов включает в себя проработку учебного материала лекций, подготовку к зачету.

Для успешного освоения дисциплины рекомендуется подробно конспектировать лекционный материал, просматривать конспекты лекций по соответствующей теме, чтобы систематизировать изучаемый материал.

При использовании дистанционных образовательных технологий и электронного обучения следует выполнять все указания преподавателя по работе на LMSплатформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Торстейнсон, П. Криптография и безопасность в технологии .NET / П. Торстейнсон, Г. А. Ганеш ; под редакцией С. М. Молявко ; перевод с английского В. Д. Хорева. — 4-е изд. — Москва : Лаборатория знаний, 2020. — 482 с. — ISBN 978-5-00101-700-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/151552. — Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
2	Информационная безопасность. Практические аспекты : учебник / Л. Х. Сафиуллина, А. Р. Касимова, Я. С. Рябов [и др.]. — Санкт-Петербург : Интермедия, 2021. — 240 с. — ISBN 9785-4383-0205-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161340. — Режим доступа: для авториз. пользователей. Скопировать в буфер
3	Защита от хакеров Web-приложений / Д. Форристал, К. Брумс, Д. Симонис, Б. Бегнолл. — Москва : ДМК Пресс, 2008. — 496 с. — ISBN 5-94074-258-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/1116. — Режим доступа: для авториз. пользователей.

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
	Электронно-библиотечная система «Лань». - Режим доступа: https://e.lanbook.com.
4	Электронный каталог Научной библиотеки Воронежского государственного университета. –
	Режим доступа: http//:www.lib.vsu.ru.
5	The Web Application Security Consortium. The WASC Threat Classification v2.0. — Элекгон.текстовые дан.—Режим доступа: http://projects.webappsec.org/w/page/13246978/Threat Classification, свободный. — Загл. с экрана.
6	The Open Web Application Security Project. — Элекгон. текстовые дан. — Режим доступа: https://www.owasp.org/index.php/Main_Page, свободный. — Загл. с экрана.
7	Безопасность интернет-приложений (01.04.02) / В.Г. Ляликова— Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru

16. Перечень учебно-методического обеспечения для самостоятельной работы

Самостоятельная работа обучающегося должна включать в себя подготовку к лабораторным работам и подготовку к промежуточной аттестации. Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован учебнометодический комплекс, который включает в себя: программу курса, учебные пособия и справочные материалы, методические указания по выполнению лабораторных работ. Студенты получают доступ к данным материалам на первом занятии по дисциплине.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий, для организации самостоятельной работы обучающихся используется онлайн-курс, размещенный на платформе Электронного университета ВГУ (LMS moodle), а также другие Интернет-ресурсы, приведенные в п.15в.

18. Материально-техническое обеспечение дисциплины:

Лекции: лекционная аудитория, учебная мебель, компьютер (ноутбук), мультимедийное оборудование (проектор, экран, средства звуковоспроизведения).

Лабораторные работы: специализированная аудитория, оснащенная учебной мебелью и персональными компьютерами для индивидуальной работы с возможностью подключения к сети «Интернет» (компьютерные классы, студии), мультимедийное оборудование (проектор, экран, средства звуковоспроизведения).

Самостоятельная работа: учебная мебель, компьютерный класс, компьютер с возможностью подключения к сети «Интернет», платформе Электронного университета ВГУ (LMS moodle).

Программное обеспечение:
- ОС Windows 10,
- интернет-браузер (Mozilla Firefox);
- ПО Adobe Reader;
- пакет стандартных офисных приложений для работы с документами, таблицами (МойОфис,LibreOffice).
- Среда разработки Visual Studio 2022
- Microsoft SQL Server 2019

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименования раздела дисциплины	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Основы Интернет безопасности	ПК-2, ПК-3	ПК-2.1, ПК-3.1, ПК-3.4	Лабораторные работы
2	Разработка ASP.NET MVC приложений			
3	Различные виды атак на web-приложения			
Промежуточная аттестация, форма контроля - зачет с оценкой				Перечень вопросов

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств: лабораторные работы.

Примеры заданий к лабораторным работам

Каждое приложение должно иметь Web архитектуру, подсистему и страницы безопасности и разграничения доступа, средства предотвращения типовых Internet атак, подсистему шифрования критически важной или персональной информации.

1. Библиотека

2. Отдел кадров
3. Распределение учебной нагрузки
4. Бронирование авиабилетов
5. Гостиница
6. Прокуратура
7. Факультет
8. ИТУ
9. Регистратура лечебного учреждения
10. Автозапчасти
11. Заказы на сборку компьютеров
12. Автосалон
13. Биржа труда
14. Турагентство
15. Аренда помещений
16. Риэлтерская фирма
17. Финансовая организация
18. Охранное агентство
19. Российский футбол
20. Альпинистский клуб
21. Управление проектами
22. Катера и яхты (аренда)
23. Ресторан
24. Платные услуги
25. Оптовые продажи

Технология проведения
Студент выполняет предложенное преподавателем задание, представляет его на дисплее, комментирует выполненные действия, анализирует и интерпретирует результаты.

Критерии оценивания

- оценивается «зачтено», если работа выполнена в полном объеме (выполнены все задания, даны пояснения);
- оценивается «не зачтено», работа выполнена не полностью или в представленной части много ошибок.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: вопросы к зачету.

Вопросы к зачету

1. Протоколы и технологии Интернет
2. Веб-серверы и Веб-браузеры. Виртуальные каталоги
3. Адресация ресурсов Интернет
4. Протоколы HTTP и HTTPS
5. Язык HTML. Основные теги
6. HTML-формы
7. Каскадные таблицы стилей
8. Язык JavaScript
9. Объектная модель документа и браузера. Примеры
10. Браузерные события
11. Серверные Веб-технологии
12. Технология ASP .NET MVC
13. Создание моделей
14. Типовые операции CRUD
15. Контроллеры
16. Представления
17. Сеансовые переменные. Куки. Сессии
18. Покупательская корзина
19. Элементы системы безопасности — аутентификация, авторизация и регистрация
20. Аутентификация с использованием ролей. Фильтры
21. Способы аутентификации в IIS
22. Безопасное хранение паролей. Алгоритмы хэширования
23. Подсистема безопасности SQL Server
24. Безопасное хранение строк соединения с БД
25. Предотвращение SQL иньекций
26. Борьба с межсайтовым скриптингом
27. Google-исследование сайтов
28. Безопасное хранение скриптов. Разрешения на виртуальные каталоги
29. Администрирование IIS. Развертывание сайтов
30. Безопасная навигация в Интернет

Критерии оценки ответов на вопросы зачета

Для оценивания результатов обучения на зачете используется 4-балльная шала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся в полной мере владеет теоретическими основами дисциплины, способен иллюстрировать ответ примерами, применять теоретические знания для решения практических задач, все лабораторные работы выполнены.	Повышенный уровень	Отлично
Обучающийся владеет теоретическими основами дисциплины, способен иллюстрировать ответ примерами, но допускает ошибки при ответе, все лабораторные работы выполнены.	Базовый уровень	Хорошо
Обучающийся частично владеет частично теоретическими основами дисциплины, фрагментарно способен иллюстрировать ответ примера и не умеет применять на практике полученные знания, все лабораторные работы выполнены.	Пороговый уровень	Удовлетворительно
Обучающийся демонстрирует отрывочные, фрагментарные знания, не ориентируется в практических задачах.	–	Неудовлетвори - тельно

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

ПК-2. Способен определять основные типы атак на web-приложения и знает методы их предотвращения. Способен анализировать научно-техническую информацию и результаты исследований.

ПК -3. Способен осуществлять разработку, анализ и обосновывать эффективность применяемых математических методов защиты информации, возникающих при работе программных и программно-аппаратных средств защиты информации при решении профессиональных, исследовательских и прикладных задач.