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

УТВЕРЖДАЮ
и.о. заведующего кафедрой
ERP-систем и бизнес-процессов
С.Л. Кенин
25.04.2022

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.В.04 Безопасность интернет-приложений

1. Код и наименование направления подготовки / специальности:

01.04.02 Прикладная математика и информатика

2. Профиль подготовки / специализация/магистерская программа:

Математическое и программное обеспечение информационных систем

3. Квалификация (степень) выпускника: магистр

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: ERP-систем и бизнес процессов

6. Составители программы: Ляликова Виктория Геннадиевна, кандидат физико-математических наук, преподаватель кафедры ERP-систем и бизнес-процессов

7. Рекомендована: НМС факультета Прикладной математики, информатики и механики № 8 от 15.04.2022

8. Учебный год: 2023/2024 **Семестр(ы):** 3

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-1	Способен проводить работы по обработке и анализу научно-технической информации, результатов исследований	ПК-1.2	Анализирует и обрабатывает информацию по тематике исследований.	Знать: способы проведения экспертной оценки функционирования и работоспособности информационных ресурсов; уметь: осуществлять руководство проектированием, проверкой работоспособности информационных ресурсов; владеть (иметь навык(и)): проведения экспертной оценки функционирования информационных ресурсов и планирование методов их реализации.
ПК-5	Способен осуществлять руководство проектированием, проверкой работоспособности информационных ресурсов (ИР), проводить экспертную оценку	ПК-5.1	Знает принципы построения архитектуры ИР, методологии и средства проектирования ИР, методы и средства проектирования интерфейсов.	Знать: принципы построения файловых систем и системного программного обеспечения инфокоммуникационной системы; уметь: проводить анализ системных проблем обработки
		ПК-5.2	Применяет принципы построения архитектуры программного	

	функционирования ИР и планирование методов их реализации		обеспечения и виды архитектур программного обеспечения, производит подготовку тестовых наборов данных, применяет методы и средства проверки работоспособности ИР.	информации на уровне инфокоммуникационной системы; владеть (иметь навык(и)): администрирования файловых систем и системного программного обеспечения инфокоммуникационной системы.

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

Форма промежуточной аттестации зачет.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоемкость (часы)				
	Всего	В том числе в интерактивной форме	По семестрам		
			№ сем. 3	№ сем.	…..
Аудиторные занятия					
в том числе: лекции	16		16		
практические	-		-		
лабораторные	32		32		
Самостоятельная работа	60		60		
Форма промежуточной аттестации	Зачет		Зачет		
Итого:	108		108		

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Введение	Терминология, статистика атак на web-ресурсы, публичность web-приложений как один из факторов повышенного внимания злоумышленников к web-ресурсам. Атака «злоупотребление функциональностью».	Безопасность интернет-приложений (01.04.02)
1.2	Атаки «грубая сила» и «переполнение буфера»	Примеры. Методы исключения атаки перебором на реальных web-приложениях	
1.3	Атака «отказ в обслуживании»	Атака «отказ в обслуживании»: классификация методов, способы	
1.4	Атака «межсайтовый скриптинг»	Примеры. Способы защиты.	
1.5	Атака «снятие отпечатков пальцев»: методы и	Примеры. Способы защиты.	

	утилиты.		
1.6	Понятие LDAP-репозитория	Понятие LDAP-репозитория (Lightweight Directory Access Protocol), методы атак на LDAP.	
1.7	Атака «инъекция команд в протоколы электронной почты»	Примеры. Способы защиты.	
1.8	Атака «навигация по запрещенным путям» Атаки «SQL-инъекция» и «XML-инъекция»	Примеры. Способы защиты.	
2. Лабораторные работы			
2.1	Атака «межсайтовый скриптинг»	Примеры по теме «Атака «межсайтовый скриптинг»» и их разбор. Выполнение задания лабораторной работы.	Безопасность интернет-приложений (01.04.02.)
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 «SQL-инъекция» и «XML-инъекция»	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	Введение	2			4	6
2	Атаки «грубая сила» и «переполнение буфера»	2		4	8	14
3	Атака «отказ в обслуживании»	2		4	8	14
4	Атака «межсайтовый скриптинг»	2		5	8	15
5	Атака «снятие отпечатков пальцев»: методы и утилиты.	2		5	8	15
6	Понятие LDAPрепозитория	2		4	8	14
7	Атака «инъекция команд в протоколы	2		5	8	15

	электронной почты»					
8	Атака «навигация по запрещенным путям» Атаки «SQL-инъекция» и «XML-инъекция»	2		5		15
	Итого:	16		32	60	108

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 LMS-платформе, 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 978-5-4383-0205-6. — 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 учебно-методический 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).

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	Введение Атаки «грубая сила» и «переполнение буфера»	ПК-1, ПК-5	ПК-1.2, ПК-5.1, ПК-5.2	Лабораторные работы
2	Атака «отказ в обслуживании»			
3	Атака «межсайтовый скриптинг»			
4	Атака «снятие отпечатков пальцев»: методы и утилиты.			
5	Понятие LDAPрепозитория			
6	Атака «инъекция команд в протоколы электронной почты»			
7	Атака «навигация по запрещенным путям» Атаки «SQL-инъекция» и «XML-инъекция»			
Промежуточная аттестация, форма контроля - зачет				Перечень вопросов

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1Текущий контроль успеваемости

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

Перечень лабораторных работ

1. Противодействие атаке «грубая сила» и «переполнение буфера»
2. Противодействие атаке «отказ в обслуживании
3. Противодействие атаке «межсайтовый скриптинг»
4. Противодействие атаке «снятие отпечатков пальцев»
5. Работа с LDAP-репозиторием
6. Противодействие атаке «инъекция команд в протоколы электронной почты»
7. Противодействие атаке «снятие отпечатков пальцев»: методы и утилиты
8. Противодействие атаке «навигация по запрещенным путям»
9. Противодействие атаке «SQL-инъекция»
10. Противодействие атаке XML-инъекция»

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.

Перечень вопросов к зачету

1. Терминология, статистика атак на web-ресурсы, публичность web-приложений как один из факторов повышенного внимания злоумышленников к web-ресурсам.
2. Атака «злоупотребление функциональностью».
3. Атаки «грубая сила» и «переполнение буфера». Примеры.
4. Методы исключения атаки перебором на реальных web-приложениях.
5. Атака «отказ в обслуживании»: классификация методов, способы защиты.
6. Атака «межсайтовый скриптинг». Примеры. Способы защиты.
7. Атака «снятие отпечатков пальцев»:методы и утилиты. Примеры. Способы защиты.
8. Понятие LDAP-репозитория (Lightweight Directory Access Protocol), методы атак на LDAP.
9. Атака «инъекция команд в протоколы электронной почты». Примеры. Способы защиты.
10. Атака «навигация по запрещенным путям». Примеры. Способы защиты.
11. Атаки «SQL-инъекция» и «XML-инъекция». Примеры. Способы защиты.

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	Удовлетвори-тельно
Обучающийся демонстрирует отрывочные, фрагментарные знания, не ориентируется в практических задачах.	–	Неудовлетвори-тельно