МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный университет»

«Утверждаю»
Заведующий кафедрой ТО и ЗИ

«31» августа 2020 г.  А.А. Сирота

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.Б.51.05 Анализ уязвимостей программного обеспечения

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

2. Профиль подготовки/специализации: анализ безопасности компьютерных систем

3. Квалификация (степень) выпускника: специалист

4. Форма образования: очная

5. Кафедра, отвечающая за реализацию дисциплины:
Кафедра технологий обработки и защиты информации

6. Составители программы:
Дрюченко Михаил Анатольевич, к.т.н., доцент

7. **Рекомендована:**
Научно-методическим советом ФКН, протокол №7 от 31 августа 2020 г.

(отметки о продлении вносятся вручную)

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

9. Цели и задачи учебной дисциплины:

Цель дисциплины – ознакомление студентов с теоретическими и практическими аспектами анализа уязвимостей и общими принципами защиты программного обеспечения (ПО) для повышения безопасности разработки и эксплуатации информационных систем различного назначения.

Основные задачи дисциплины:

- ознакомление студентов с причинами возникновения и принципами эксплуатации уязвимостей в программном коде, изучение практических примеров уязвимостей в программном коде;
- изучение принципов анализа кода, внутреннего представления программы для анализа, ознакомление с принципами работы статистических и динамических анализаторов кода;
- изучение принципов создания безопасного ПО и современных методов защиты исходных и байт кодов программ;
- овладение практическими навыками формирования комплекса мер для повышения качества разработки ПО.

10. Место учебной дисциплины в структуре ООП:

Учебная дисциплина «Анализ уязвимостей программного обеспечения» относится к блоку обязательных дисциплин обще-профессиональной части.

Для успешного освоения дисциплины необходимы входные знания в области устройства ЭВМ и операционных систем, теории компиляторов, информатики и математических основ криптографии.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Компетенция		Планируемые результаты обучения
Код	Название	
ОПК-8	способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач	**знать:** принципы работы отладчиков, дизассемблеров, статических и динамических анализаторов кода, теоретические и практические аспекты появления уязвимостей, принципы работы современных методов защиты ПО; **уметь:** использовать современные средства разработки для реализации безопасного ПО; **владеть:** практическими навыками грамотной разработки и использования современных средств отладки, дизассемблирования программ.
ПСК-1.1	способностью проводить анализ защищенности и находить уязвимости компьютерной системы	**знать:** методы обнаружения и предотвращения типичных уязвимостей (переполнения буфера, уязвимости форматной строки и т.п.), аспекты защиты ПО, принципы обфускации кода; **уметь**: применять на практике полученные знания и навыки для анализа программного обеспечения на наличие уязвимостей (экспертиза исходного кода и файззинг-тестирование), локализации их последствий, устранения самих уязвимостей, решения задач защиты программного кода; **владеть**: практическими навыками проведения экспертизы исходного кода, отладки, статического и динамического анализа кода.

12. Объем дисциплины в зачетных единицах/час — 4/144.
Форма промежуточной аттестации: *зачет с оценкой*.

13. Виды учебной работы:

Вид учебной работы	Трудоемкость (часы)	
	Всего	По семестрам

		№ сем. А	№ сем.	Итого
Аудиторные занятия	48	48		48
в том числе: лекции	24	24		24
практические	-	-		-
лабораторные	24	24		24
Самостоятельная работа	96	96		96
Форма промежуточной аттестации *(зачет – __ час. / экзамен – __час.)*	-	-		-
Итого:	144	144		144

13.1 Содержание дисциплины:

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1. Лекции		
1.1	Теоретические аспекты возникновения уязвимостей	Понятие и классификация уязвимостей. Причины возникновения уязвимостей в программном коде и принципы их эксплуатации. Уязвимости переполнения буфера в стеке и куче. Методы обнаружения и предотвращения переполнения буфера. Уязвимость форматной строки. Уязвимость переполнения целых чисел. Эксплойты.
1.2	Практические аспекты анализа уязвимостей	Практические примеры уязвимостей в программном коде. Типовые сценарии выявления уязвимостей в программном коде. Статические и динамические анализаторы кода. Тестирование по принципу «белого ящика». Файззингтестирование. Повышение качества разработки ПО при использовании специализированных программных средств.
1.3	Методы защиты программного обеспечения	Принципы создания безопасного ПО. Современные методы защиты ПО от взлома. Технические меры защиты ПО. Защита кода от анализа. Принципы работы обфускаторов исходных и байткодов.
2. Практические занятия		
2.1	нет	
3. Лабораторные работы		
3.1	Теоретические аспекты возникновения уязвимостей	1. Изучение принципов действия атаки переполнения буфера, реализация на практике модели атаки переполнения буфера в стеке и куче. 2. Исследование уязвимостей форматной строкой, реализация на практике модели атаки с использованием данной уязвимости. 3. Исследование уязвимости переполнения целых.
3.2	Практические аспекты анализа уязвимостей	4. Изучение принципов работы статических анализаторов исходного кода. 5. Изучение принципов динамического анализа кода.
3.3	Методы защиты программного обеспечения	6. Изучение принципов защиты и обфускации исходного и байт кода.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Сам. работа	Всего
1	Теоретические аспекты возникновения уязвимостей в программном коде	8	8	36	52
2	Практические аспекты анализа уязвимостей	8	10	30	48
3	Методы защиты программного обеспечения	8	6	30	44

Итого:	24	24	96	144

14. Методические указания для обучающихся по освоению дисциплины

(рекомендации обучающимся по освоению дисциплины: работа с конспектами лекций, презентационным материалом, выполнение практических заданий, тестов, заданий текущей аттестации и т.д.)

1) При изучении дисциплины рекомендуется использовать следующие средства**:**

- рекомендуемую основную и дополнительную литературу;
- методические указания и пособия;
- контрольные задания для закрепления теоретического материала;
- электронные версии учебников и методических указаний для выполнения лабораторно - практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, решение задач) студентов по материалам лекций и практических работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала. Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

3) При проведении лабораторных занятий обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка методов, алгоритмов и технологий обработки информации, излагаемых в рамках лекций.

4) При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей, вовремя подключаться к online занятиям, ответственно подходить к заданиям для самостоятельной работы.

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

(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)

а) основная литература:

№ п/п	Источник
1	Практикум по курсу "Разработка приложений на C++" [Электронный ресурс] : учебно-методическое пособие : [для студ. фак. компьютер. наук очной формы обучения для направлений: 09.04.02 - Информационные системы и технологии, 09.03.02 - Информационные системы и технологии, 10.03.01 - Информационная безопасность; специальность 10.05.01 - Компьютерная безопасность] / Воронеж. гос. ун-т ; сост.: М.А. Дрюченко, Е.Ю. Митрофанова .— Электрон. текстовые дан. — Воронеж : Издательский дом ВГУ, 2018 .— Загл. с титула экрана .— Свободный доступ из интрасети ВГУ .— Текстовый файл .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m18-158.pdf>.
2	Страуструп, Бьерн. Язык программирования C++. Специальное издание = The C++ programming language. Special edition. / Бьерн Страуструп ; пер. с англ. под ред. Н.Н. Мартынова .— Москва : Бином, 2015 .— 1135 с. : ил .— Предм. указ.: с.1117-1135 .— ISBN 978-5-7989-0425-9 .— ISBN 0-201-70073-5.

б) дополнительная литература:

№ п/п	Источник
3	*Щербаков, Андрей Юрьевич. Современная компьютерная безопасность. Теоретические основы. Практические аспекты : учебное пособие для студ. вузов / А.Ю. Щербаков .— М. : Кн. мир, 2009 .— 351, [1] с. : ил., табл. — (Высшая школа) .— Библиогр.: с.350-351 .— ISBN 978-5-8041-0378-2.*
4	Хогланд Г. Взлом программного обеспечения : Анализ и использование кода / Г. Хогланд, Г. Мак-Гроу. – М. : Вильямс, 2005. - 400 с.
5	Козиол Дж. Искусство взлома и защиты систем / Дж. Козиол, Д. Личфилд, Д. Эйтэл ; редакторы, переводчики, составители: Е. Матвеев. – СПб [и др.] : Питер, 2006. – 416 с.
6	Ховард М. 19 смертных грехов, угрожающих безопасности программ. Как не допустить типичных ошибок : пер. с англ. / М. Ховард, Д. Лебланк, Д. Виега. – М. : ДМК Пресс, 2006. – 287 с.

в)информационные электронно-образовательные ресурсы (официальные ресур-

сы интернет)*:

№ п/п	Ресурсы Интернет
7	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
8	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
9	ЭБС «Издательства «Лань», Договор №3010-06/71-14 от 25.11.2014, ЭБС «Университетская библиотека online», Договор №3010-06/70-14 от 25.11.14, Национальный цифровой ресурс «РУКОНТ», Договор №ДС-208 от 01.02.2012

* Вначале указываются ЭБС, с которыми имеются договора у ВГУ, затем открытые электронно-образовательные ресурсы

16. Перечень учебно-методического обеспечения для самостоятельной работы

(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)

№ п/п	Источник
1	Щербаков, Андрей Юрьевич. Современная компьютерная безопасность. Теоретические основы. Практические аспекты : учебное пособие для студ. вузов / А.Ю. Щербаков .— М. : Кн. мир, 2009 .— 351, [1] с. : ил., табл. — (Высшая школа) .— Библиогр.: с.350-351 .— ISBN 978-5-8041-0378-2.

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

Для реализации учебного процесса используется:

ПО Microsoft в рамках подписок «Imagine»,ежегодные сублицензионные договоры № 56035/BPH3739 и № 56036/BPH3739 от 07.10.2016.

При реализации дисциплины могут использоваться технологии электронного обучения и дистанционные образовательные технологии на базе портала edu.vsu.ru, а также другие доступные ресурсы сети Интернет.

18. Материально-техническое обеспечение дисциплины:

(при использовании лабораторного оборудования указывать полный перечень, при большом количестве оборудования можно вынести данный раздел в приложение к рабочей программе)

1) Мультимедийная лекционная аудитория (корп.1а, ауд. № 380), ПК-Intel-G3420, рабочее место преподавателя: проектор, видеокоммутатор, специализированная мебель: доска меловая 1 шт., столы 31 шт., стулья 64 шт.; выход в Интернет, доступ к фондам учебно-методической документации и электронным изданиям.

2) Компьютерный класс (один из корп. 1а, ауд. № 291, 293, 295, 387, 381), ПК-Intel-Core2/i3 14 шт., специализированная мебель: доска маркерная 1 шт., столы 14 шт., стулья 28 шт.; доступ к фондам учебно-методической документации и электронным изданиям, доступ к электронным библиотечным системам, выход в Интернет.

19. Фонд оценочных средств:

19.1 Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС* (средства оценивания)
ОПК-8 способностью использовать языки и системы программирования,	Знать принципы работы отладчиков, дизассемблеров, статических и динамических анализа-	Разделы 1-3 Теоретические аспекты возникновения уязвимостей. Практические ас-	Устный опрос, Лабораторные работы 1-6

инструментальные средства для решения профессиональных, исследовательских и прикладных задач	торов кода, теоретические и практические аспекты появления уязвимостей, принципы работы современных методов защиты ПО	пекты анализа уязвимостей. Методы защиты программного обеспечения	
	Уметь использовать современные средства разработки для реализации безопасного ПО	Разделы 1,2 Теоретические аспекты возникновения уязвимостей. Практические аспекты анализа уязвимостей	Лабораторные работы 1-6
	Владеть практическими навыками грамотной разработки и использования современных средств отладки, дизассемблирования программ	Разделы 1,2 Теоретические аспекты возникновения уязвимостей. Практические аспекты анализа уязвимостей	Лабораторные работы 1-6
ПСК-1.1 способностью проводить анализ защищенности и находить уязвимости компьютерной системы	Знать методы обнаружения и предотвращения типичных уязвимостей (переполнения буфера, уязвимости форматной строки и т.п.), аспекты защиты ПО, принципы обфускации кода	Разделы 1-3 Теоретические аспекты возникновения уязвимостей. Практические аспекты анализа уязвимостей. Методы защиты программного обеспечения	Тест по соответствующим разделам, Лабораторные работы 1-6
	Уметь применять на практике полученные знания и навыки для анализа программного обеспечения на наличие уязвимостей (экспертиза исходного кода и файззингтестирование), локализации их последствий, устранения самих уязвимостей, решения задач защиты программного кода	Разделы 2,3 Практические аспекты анализа уязвимостей. Методы защиты программного обеспечения	Лабораторные работы 1-6
	Владеть практическими навыками проведения экспертизы исходного кода, отладки, статического и динамического анализа кода	Разделы 2,3 Практические аспекты анализа уязвимостей. Методы защиты программного обеспечения	Лабораторные работы 1-6

*В графе «ФОС» в обязательном порядке перечисляются оценочные средства текущей и промежуточной аттестаций

19.2. Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Для оценивания результатов обучения используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1) знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;

2) умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу;

3) владение навыками программирования, использования современных программных средств разработки и отладки программ.

4) владение навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования специализированных утилит статического и динами-

ческого анализа кода.

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций) на государственном экзамене:

- высокий (углубленный) уровень сформированности компетенций;
- повышенный (продвинутый) уровень сформированности компетенций;
- пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на государственном экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Для оценивания результатов обучения на зачете используется – зачтено, не зачтено по результатам тестирования.

Соотношение показателей, критериев и шкалы оценивания результатов обучения на государственном экзамене представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок (зачет с оценкой)

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	Неудовлетворительно

19.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

19.3.1 Примерный перечень применяемых оценочных средств

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Контрольная работа по разделам дисциплины	Теоретические вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной в разделе 19.2
3	Тест	Содержит 40 тестовых вопроса, за правильный ответ	оценка «отлично» выставляется студенту, если количество пра-

		на каждый из которых дается 1 балл.	вильных ответов составляет 36-40, оценка «хорошо» – 31-35, оценка «удовлетворительно» – 23-30, оценка «неудовлетворительно» – 22 и менее.
4	Лабораторная работа	Содержит 6 лабораторных задания, предусматривающие разработку и исследование программ, содержащих типовые классы уязвимостей	При успешном выполнении работы осуществляется допуск к зачету
5	КИМ промежуточной аттестации	Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает 2 заданий вопросов для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции.	Шкалы оценивания приведены в разделе 19.2

19.3.2. Примерный перечень вопросов к зачету с оценкой

№	Содержание
1	Классификация уязвимостей ПО
2	Уязвимость переполнения буфера в стеке
3	Уязвимость переполнения буфера в куче
4	Уязвимость переполнения целых
5	Уязвимость форматной строкой
6	Методы обнаружения уязвимостей. Тестирование по принципу «белого ящика»
7	Методы обнаружения уязвимостей. Тестирование по принципу «черного ящика»
8	Динамический анализ кода, фаззингтестирование
9	Проблемы безопасности ПО, связанные с компиляторной оптимизацией
10	Принципы создания безопасного ПО, ГОСТ Р56939-2016
11	Методы защиты ПО от взлома
12	Технические меры защиты ПО
13	Приемы обфускации
14	Динамическое ветвление и контекстная зависимость
15	Динамические анализаторы кода
16	Средства отладки и взлома программ
17	Обфускация абстрактных данных
18	Обфускация кода на этапе дизассемблирования

19.3.3. Пример задания для выполнения лабораторной работы

Лабораторная работа №1

«Исследование атаки переполнения буфера»

Цель работы: изучение принципов действия атаки переполнения буфера. Реализация на практике модели атаки переполнения буфера в стеке.
Форма контроля: отчет в электронном виде
Количество отведенных аудиторных часов: 6
Задание: На языке Си написать следующие программы:

- уязвимую программу, подверженную переполнению буфера в стеке;
- программу, защищенную от переполнения;
- программу, реализующую атаку переполнения буфера;
- программу эксплойт.

Примеры контрольных вопросов:

1. Что такое уязвимости?

2. Каковы причины возникновения уязвимостей в программном коде?
3. Как эксплуатируются уязвимости?

19.3.4. Пример контрольно-измерительного материала

УТВЕРЖДАЮ
Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота
__.__.2020

Направление подготовки / специальность 10.05.01 Компьютерная безопасность

Дисциплина Б1.Б.51.05 Анализ уязвимостей программного обеспечения

Форма обучения Очное

Вид контроля Зачет с оценкой

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Классификация уязвимостей ПО
2. Статические анализаторы кода

Преподаватель _____ М.А. Дрюченко

19.3.5. Пример заданий теста по разделам дисциплины

В приведенных фрагментах кода найти и исправить ошибки (потенциальные уязвимости)

1	`void encryptData(char *str)`
	`{`
	`  char pwd[64];`
	`  if(getPassword(pwd, sizeof(pwd)))`
	`  ...`
	`  ZeroMemory(pwd, sizeof(pwd));`
	`}`	

2	`int main(int argc, char *argv[])`
	`{`
	`  char login[100], pwd[100];`
	`  int pwd_len;`
	
	`  strcpy(login, argv[1]);`
	`  strcpy(pwd,  argv[2]);`
	`  pwd_len = atoi(argv[3]);`
	
	`  // флаг, дающий права администратора`
	`  int admin = 0;`
	`  char orig_pwd[100] = "123456";`
	
	`  if(pwd_len < 1) pwd_len = 0;`
	`  pwd_len++;`
	`  if(login = "admin")`
	`  {`
	`  admin = 1;`
	`  for(i=0; i<= pwd_len; i++)`
	`  {`
	`  if((pwd[i])!=orig_pwd[i])admin=0;`
	`  }`
	`  }`	

	`    setStastus(admin);` `}`	

3	`bool finished = false;`
	`char *buf = (char*)malloc(BUF_SIZE);`
	`...`
	`if(finished)`
	`    free(buf);`
	`...`
	`free(buf);`	

4	`char *buf1, *buf2;`
	`buf1 = (char*)malloc(size);`
	`...`
	`buf2 = (char*)malloc(size);`
	`strncpy(buf2, buf1, size);`	

	`...`	

19.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок.

Промежуточная аттестация может включать в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

При оценивании используется количественная шкала. Критерии оценивания приведены выше в таблице раздела 19.2.