Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

Сирота Александр Анатольевич

Кафедра технологий обработки и защиты информации

29.06.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.53 Анализ уязвимостей и защита программного обеспечения

1. Код и наименование направления подготовки/специальности:

10.03.01 Информационная безопасность

2. Профиль подготовки/специализация:

Безопасность компьютерных систем

3. Квалификация (степень) выпускника:

Бакалавриат

4. Форма обучения:

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:

протокол №5 от 10.03.21

8. Учебный год:

2024-2025

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:

Блок обязательные дисциплины вариативной 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) и индикаторами их достижения:

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями;	ОПК-1.4.3 знает источники угроз информационной безопасности в компьютерных системах и сетях и меры по их предотвращению	Знает источники угроз информационной безопасности в компьютерных системах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамического анализа кода, методы устранения уязвимостей. Умеет применять на практике полученные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза исходного кода, статический и динамический анализ, файззингтестирование). Владеет практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования специализированных утилит статического и динамического анализа кода.
ОПК-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями;	ОПК-1.4.4 умеет анализировать угрозы безопасности информации в компьютерных системах и сетях	Знает известные методы анализа ПО на наличие уязвимостей, методы статического и динамического анализа программ, методы проведения экспертизы исходного кода. Умеет применять на практике полученные знания и навыки для анализа ПО на наличие уязвимостей. Владеет специализированными инструментами и практическими навыками анализа ПО на наличие уязвимостей.

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями;	ОПК-1.4.5 знает принципы функционирования программных средств криптографической защиты информации	Знает принципы функционирования программных средств криптографической защиты информации. Владеет практическими навыками разработки, использования (известных криптографических библиотек) и тестирования специализированных алгоритмов и ПО, реализующих криптографические методы и алгоритмы.

12. Объем дисциплины в зачетных единицах/час:

3/108

Форма промежуточной аттестации:

Зачет с оценкой,Контрольная работа

13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 8	Всего
Аудиторные занятия	48	48
Лекционные занятия	12	12
Практические занятия		0
Лабораторные занятия	36	36
Самостоятельная работа	60	60
Курсовая работа		0
Промежуточная аттестация	0	0
Часы на контроль		0
Всего	108	108

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1.1	Теоретические аспекты возникновения уязвимостей	1. Понятие и классификация уязвимостей. 2. Причины возникновения уязвимостей в программном коде и принципы их эксплуатации. 3. Уязвимости переполнения буфера в стеке. 4. Уязвимости переполнения буфера в куче. 5. Методы обнаружения и предотвращения переполнения буфера. 6. Уязвимость форматной строки. 7. Уязвимость переполнения целых чисел. 8. Эксплойты.	Создан онлан электронный курс, размещены материалы к лекции. Размещены индивидуальные задания для выполнения лабораторных работ.
1.2	Практические аспекты анализа уязвимостей	9. Практические примеры уязвимостей в программном коде. 10. Типовые сценарии выявления уязвимостей в программном коде. 11. Статические и динамические анализаторы кода. 12. Тестирование по принципу «белого ящика». 13. Файззингтестирование. 14. Повышение качества разработки ПО при использовании специа-лизированных программных средств.	Создан онлан электронный курс, размещены материалы к лекции. Размещены индивидуальные задания для выполнения лабораторных работ.

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1.3	Методы защиты программного обеспечения	15. Принципы создания безопасного ПО. 16. Современные методы защиты ПО от взлома. 17. Технические меры защиты ПО. 18. Защита кода от анализа. 19. Принципы работы обфускаторов исходных и байткодов.	Создан онлан электронный курс, размещены материалы к лекции. Размещены индивидуальные задания для выполнения лабораторных работ.
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.	Размещены индивидуальные задания для выполнения лабораторных работ.
3.2	Практические аспекты анализа уязвимостей	4. Изучение принципов работы статических анализаторов исходного кода. 5. Изучение принципов динамического анализа кода.	Размещены индивидуальные задания для выполнения лабораторных работ.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Теоретические аспекты возникновения уязвимостей	5		8	20	33
2	Практические аспекты анализа уязвимостей	4		20	20	44
3	Методы защиты программного обеспечения	3		8	20	31
		12	0	36	60	108

14. Методические указания для обучающихся по освоению дисциплины

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

№ п/п	Источник
1	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.
2	Дрюченко, Михаил Анатольевич. Разработка приложений на C++ : учебно-методическое пособие / М.А. Дрюченко, Е.Ю. Митрофанова ; Воронеж. гос. ун-т .— Воронеж : Издательский дом ВГУ, 2019 .— 114 с. — Библиогр.: с. 114.

б) дополнительная литература:

№ 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.
2	Хогланд Г. Взлом программного обеспечения : Анализ и использование кода / Г. Хогланд, Г. Мак-Гроу. – М. : Вильямс, 2005. - 400 с.
3	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.
4	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:

№ п/п	Источник
1	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
2	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
3	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

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ 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. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

Для реализации учебного процесса используется: ПО Microsoft в рамках подписки "Imagine/Azure Dev Tools for Teaching", договор №3010-16/96-18 от 29 декабря 2018г.

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:

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. Оценочные средства для проведения текущей и промежуточной аттестаций

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

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	Разделы 1-3 Теоретические аспекты возникновения уязвимостей. Практические аспекты анализа уязвимостей. Методы защиты программного обеспечения.	ОПК-1.4	ОПК-1.4.3	Контрольная работа по соответствующим разделам. Лабораторные работы 1-5
2	Разделы 1-3 Теоретические аспекты возникновения уязвимостей. Практические аспекты анализа уязвимостей. Методы защиты программного обеспечения.	ОПК-1.4	ОПК-1.4.4	Контрольная работа по соответствующим разделам. Лабораторные работы 1-5

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
3	Разделы 1-3 Теоретические аспекты возникновения уязвимостей. Практические аспекты анализа уязвимостей. Методы защиты программного обеспечения.	ОПК-1.4	ОПК-1.4.5	Контрольная работа по соответствующим разделам. Лабораторные работы 1-5

Промежуточная аттестация

Форма контроля - Зачет с оценкой,Контрольная работа

Оценочные средства для промежуточной аттестации

Перечень вопросов, практическое задание

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Текущий контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Устный опрос на практических занятиях

Контрольная работа по теоретической части курса

Лабораторные работы

Примерный перечень применяемых оценочных средств

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	Устный опрос на практических занятиях	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 ниже
3	Лабораторная работа	Содержит 5 лабораторных заданий, предусматривающие разработку и исследование программ, содержащих типовые классы уязвимостей	При успешном выполнении работ в течение семестра фиксируется возможность оценивания только теоретической части дисциплины в ходе промежуточной аттестации (экзамена), в противном случае проверка задания по лабораторным работам выносится на зачет.

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: *4*

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?

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);	

	...	

20.2 Промежуточная аттестация

Промежуточная аттестация может включать в себя проверку теоретических вопросов, а также, при необходимости (в случае невыполнения в течение семестра), проверку выполнения установленного перечня лабораторных заданий, позволяющих оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

Для оценки теоретических знаний используется перечень контрольно-измерительных материалов.

Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает два задания - вопросов для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции. При оценивании используется количественная шкала. Критерии оценивания приведены в таблице ниже.

Для оценивания результатов обучения на экзамене 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 динамического анализа кода.

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

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

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

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. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	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. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	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. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки. Не выполнены лабораторные работы в соответствии с установленным перечнем.	–	Неудовлетворительно

Примерный перечень вопросов к зачету

№	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 Р569392016*
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

Пример контрольно-измерительного материала

УТВЕРЖДАЮ

Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота

__.__.2021

Направление подготовки / специальность 10.03.01 Информационная безопасность

Дисциплина Б1.О.53 Анализ уязвимостей и защита 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