Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе и образовательным инновациям
_____ О.Н. Здрок
«02» июля 2021 г.

Регистрационный № УД – 10418/уч.

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ

Учебная программа учреждения высшего образования по учебной дисциплине для специальности:

1-98 01 01 Компьютерная безопасность (по направлениям)
Направление специальности
1-98 01 01-01 Компьютерная безопасность (математические методы и программные системы)

2021 г.

Учебная программа составлена на основе ОСВО 1-98 01 01-2013 и учебных планов № Р 98-138/уч., № Р 98и-141/уч. от 30.05.2013.

СОСТАВИТЕЛИ:

Курбацкий А.Н., заведующий кафедрой технологий программирования факультета прикладной математики и информатики Белорусского государственного университета, доктор технических наук, профессор;

Федчук А.В., старший преподаватель кафедры технологий программирования факультета прикладной математики и информатики Белорусского государственного университета.

РЕЦЕНЗЕНТ:

Леванцевич В.А., старший преподаватель кафедры программного обеспечения информационных технологий УО «Белорусский государственный университет информатики и радиоэлектроники».

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой технологий программирования Белорусского государственного университета
(протокол № 16 от 28.05.2021);

Советом факультета прикладной математики и информатики БГУ
(протокол № 11 от 22.06.2021).

Заведующий кафедрой
технологий программирования _____ А.Н. Курбацкий

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи учебной дисциплины

Цель учебной дисциплины – ознакомление студентов с современными подходами в обеспечении информационной безопасности в операционных системах (ОС), изучение архитектурных решений и практических приложений концепций безопасности.

Задачи учебной дисциплины:

1. Изучение подходов и методов обеспечения безопасности программного обеспечения (ПО) в современных операционных системах и безопасности операционных систем.
2. Формирование практических умений и навыков безопасной разработки программного обеспечения.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием.

Учебная дисциплина относится **к циклу** дисциплин специализации компонента учреждения высшего образования. В современном информационном обществе существует востребованность в специалистах по безопасному программированию, владеющими инструментами анализа кода, локальных уязвимостей, используя различные алгоритмы противодействия обхода механизмов безопасности.

Программа составлена с учетом **межпредметных связей** с учебными дисциплинами. Основой для изучения учебной дисциплины являются учебные дисциплины I ступени высшего образования «Программирование», «Операционные системы», «Архитектура компьютеров», «Компьютерные сети», «Криптографические методы».

Требования к компетенциям

Освоение учебной дисциплины «Безопасность операционных систем» должно обеспечить формирование следующих академических, социально-личностных и профессиональных компетенций:

академические компетенции:

АК-1. Уметь применять базовые научно-теоретические знания для решения теоретических и практических задач.

АК-2. Владеть системным и сравнительным анализом.

ЛК-3. Владеть исследовательскими навыками.

АК-4. Уметь работать самостоятельно.

АК-5. Быть способным вырабатывать новые идеи.

АК-9. Уметь учиться, повышать свою квалификацию в течение всей жизни.

социально-личностные компетенции:

СЛК-3. Обладать способностью к межличностным коммуникациям.

СЛК-6. Уметь работать в команде.

профессиональные компетенции:

ПК-1. Работать с научной, нормативно-справочной и специальной литературой с целью получения последних сведений о новых методах защиты информации, о стойкости существующих систем защиты информации.

ПК-2. Формулировать задачи, возникающие при организации защиты информации.

ПК-3. Разрабатывать модели явлений, процессов или систем при организации защиты информации.

ПК-4. Выбирать необходимые методы исследования, модифицировать существующие, разрабатывать новые методы и применять их для решения поставленных задач при организации защиты информации.

ПК-5. Выполнять оценку эффективности методов защиты информации.

ПК-12. Пользоваться глобальными информационными ресурсами.

ПК-13. Владеть современными средствами телекоммуникаций.

ПК-14. Знать и применять на практике национальное законодательство по защите информации.

ПК-16 Разрабатывать техническое задание на разработку средств и систем защиты информации.

ПК-18. Разрабатывать программные, аппаратно-программные и технические средства и системы защиты информации; разрабатывать необходимую документацию.

ПК-19. Выполнять оценку безопасности реализации средств и систем защиты информации.

ПК-21. Эксплуатировать программные, аппаратно-программные и технические средства и системы защиты информации; осуществлять контроль за их использованием; вести необходимую для этого документацию.

ПК-26 Оценивать конкурентоспособность и экономическую эффективность разрабатываемых технологий.

В результате освоения учебной дисциплины студент должен:

знать:

- терминологию и понятия информационной безопасности;
- архитектуру и внутреннее устройство операционных систем;
- устройство подсистем информационной безопасности в ОС.

уметь:

- оценивать эффективность защиты данных;
- обеспечивать критерии информационной безопасности в приложениях и операционных системах.

владеть:

- навыками создания безопасного программного обеспечения;
- навыками использования методов защиты информации в современных ОС.

Структура учебной дисциплины

Дисциплина изучается в седьмом семестре. Всего на изучение учебной дисциплины «Безопасность операционных систем» отведено:

– для очной формы получения высшего образования – 159 часов, в том числе 68 аудиторных часов, из них: лекции – 34 часов, лабораторные занятия – 30 часов (в том числе — 12 часов дистанционного обучения с применением ИКТ), управляемая самостоятельная работа – 4 часа дистанционного обучения с применением ИКТ.

Трудоемкость учебной дисциплины составляет 4 зачетные единицы.

Форма текущей аттестации – зачет, экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1. Защищенное программирование

Тема 1.1. Введение в информационную безопасность
Введение в дисциплину и терминология. Стандарты информационной безопасности. Оценка рисков информационной безопасности.

Тема 1.2. Основы безопасного программирования
Безопасное программирование. Инструменты анализа кода.

Раздел 2. Механизмы безопасности операционных систем

Тема 2.1. Механизмы безопасности ОС семейства Windows
Контроль и аудит доступа в ОС Windows. Привилегии, токены, имперсонация. Механизм User Account Control. Подсистема WSL. Системные программы в Windows.

Тема 2.2. Механизмы безопасности ОС семейства Unix/Linux
Контроль и аудит доступа в ОС Linux. Команда sudo. Информационная безопасность в macOS. Парольные политики в Linux.

Тема 2.3. Информационная безопасность в мобильных ОС
Архитектура ОС Android. Разрешения в Android. Архитектура ОС iOS. Разрешения в iOS. Особенности ОС на встраиваемых и носимых устройствах.

Раздел 3. Исследование безопасности информационных систем

Тема 3.1. Инструменты сбора информации и анализа уязвимостей
Инструменты сбора информации. Инструменты анализа локальных уязвимостей. Фреймворк Metasploit.

Тема 3.2. Инструменты анализа сетевых уязвимостей и методы защиты
Инструменты анализа трафика и сетевых уязвимостей. Противодействие обходу механизмов безопасности.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Дневная форма получения образования с применением дистанционных образовательных технологий

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
1	**Защищенное программирование**	**8**			**6**		**2 (ДО)**	
1.1	Введение в информационную безопасность	2			2			устный опрос
1.2	Основы безопасного программирования	6			4		2 (ДО)	отчет
2	**Механизмы безопасности операционных систем**	**18**			**8** **8 (ДО)**		**2 (ДО)**	
2.1	Механизмы безопасности ОС семейства Windows	8			4 4 (ДО)			тест, отчет
2.2	Механизмы безопасности ОС семейства Linux	4			4			отчет
2.3	Информационная безопасность в мобильных ОС	6			4 (ДО)		2 (ДО)	тест, отчет
3	**Исследование безопасности информационных систем**	**8**			**4** **4 (ДО)**			
3.1	Инструменты сбора информации и анализа уязвимостей	4			4 (ДО)			коллоквиум, устный опрос
3.2	Инструменты анализа сетевых уязвимостей и методы защиты	4			4			отчет
	Всего	**34**			**30**		**4**	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень основной литературы

1. Макконнелл С. Совершенный код. СПб.: БХВ-Петербург, 2017, 896 с.
2. Рихтер Дж. Windows через C/C++. М.: Русская Редакция, 2009, 896 с.
3. Руссинович М., Соломон Д., Ионеску А., Йосифович П. Внутреннее устройство Windows. Седьмое издание. СПб.: Питер, 2018, 944 с.
4. Таненбаум Э., Бос Х. Современные операционные системы. СПб.: Питер, 2018, 1120 с.
5. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходный код на С. М.: Вильямс, 2016. 1024 с.
6. Юричев Д. Reverse Engineering. 2020, 1039 с.

Перечень дополнительной литературы

1. Рябко Б, Фионов А. Криптография в информационном мире. М.: ГЛ-Телеком, 2019, 300 с.
2. Олифер В., Олифер Н. Компьютерные сети. СПб.: Питер, 2020, 1009 с.

Перечень рекомендуемых средств диагностики и методика формирования итоговой оценки

Для диагностики компетенций в рамках учебной дисциплины рекомендуется использовать следующие формы:

1) Устная форма: устный опрос, коллоквиум.
2) Письменная форма: тест, отчет с оцениванием на основе модульно-рейтинговой системы.

Формой текущей аттестации по дисциплине «Безопасность информационных систем» учебным планом предусмотрен зачет и экзамен.

При формировании итоговой оценки используется рейтинговая оценка знаний студента, дающая возможность проследить и оценить динамику процесса достижения целей обучения. Рейтинговая оценка предусматривает использование весовых коэффициентов для текущего контроля знаний и текущей аттестации студентов по дисциплине.

Примерные весовые коэффициенты, определяющие вклад текущего контроля знаний в рейтинговую оценку:

- отчет – 50 %;
- тест – 20%;
- устный опрос – 20 %;
- коллоквиум – 10 %.

Рейтинговая оценка по дисциплине рассчитывается на основе оценки текущей успеваемости и экзаменационной оценки с учетом их весовых коэффициентов. Весовой коэффициент оценки по текущей успеваемости составляет 40 %, экзаменационной оценки – 60 %.

Примерный перечень заданий для управляемой самостоятельной работы студентов

Управляемая самостоятельная работа (консультационно-методическая поддержка и контроль) осуществляться преимущественно в дистанционной форме и обеспечивается средствами образовательного портала БГУ (LMS Moodle).

В отдельных случаях управляемая самостоятельная работа проводится в форме аудиторных занятий, согласно утвержденному графику.

Объем часов на составление и размещение заданий, консультации и контроль, осуществляемые с использованием технологий дистанционного обучения, планируется в пределах учебных часов, отведенных на УСР.

Тема 1.2. Основы безопасного программирования (2 ч/ДО)

Безопасное программирование. Инструменты анализа кода.

Обсуждение и анализ эволюции средств контроля кода. Предложить варианты автоматического обнаружения ошибок в коде и небезопасного программирования.

(Форма контроля –отчет).

Тема 2.3. Информационная безопасность в мобильных ОС (2 ч/ДО)
Архитектура ОС Android. Разрешения в Android. Архитектура ОС iOS. Разрешения в iOS. Особенности ОС на встраиваемых и носимых устройствах. Анализ сходств и различий в подходах к информационной безопасности в мобильных и встраиваемых ОС. Демонстрация различий с помощью приложений, использующих уникальные возможности по обеспечению ИБ. (Форма контроля – отчет, тест).

Примерная тематика лабораторных занятий

Лабораторная работа № 1. Реализация приложения с использованием методик безопасного программирования и средств автоматического контроля качества кода.

Лабораторная работа № 2. Использование принципа наименьших привилегий в ОС Windows через User Account Control

Лабораторная работа № 3. Управление правами пользователя и ACL в ОС Linux

Лабораторная работа № 4. Разработка мобильного приложения с использованием стандарта MSTG

Лабораторная работа № 5. Разработка приложения с полезной нагрузкой с использованием фреймворка Metasploit.

Рекомендуемая тематика коллоквиума:

Коллоквиум «Способы обеспечения информационной безопасности в настольных операционных системах (Windows, Linux, macOS)».

Текущий контроль знаний проводится в соответствии с учебно-методической картой дисциплины.

Описание инновационных подходов и методов к преподаванию учебной дисциплины

При организации образовательного процесса используются ***метод анализа конкретных ситуаций (кейс-метод) и метод проектного обучения***.

Кейс-метод предполагает:

- приобретение студентом знаний и умений для решения практических задач в области обеспечения безопасности операционных систем;
- анализ ситуации, используя профессиональные знания, собственный опыт, дополнительную литературу и иные источники по теме дисциплины.

Метод проектного обучения обеспечивает:

- способ организации учебной деятельности студентов, развивающий актуальные для учебной и профессиональной деятельности навыки планирования, самоорганизации, сотрудничества и предполагающий создание собственного продукта;

- приобретение навыков для решения исследовательских, творческих, социальных, предпринимательских и коммуникационных задач.

Методические рекомендации по организации самостоятельной работы обучающихся

Для организации самостоятельной работы студентов по учебной дисциплине следует использовать современные информационные ресурсы: разместить на образовательном портале комплекс учебных и учебно-методических материалов (учебно-программные материалы, учебное издание для теоретического изучения дисциплины, методические указания к лабораторным занятиям, материалы текущего контроля и текущей аттестации, позволяющие определить соответствие учебной деятельности обучающихся требованиям образовательных стандартов высшего образования и учебно-программной документации, в т.ч. вопросы для подготовки к зачету, задания, тесты, вопросы для самоконтроля, тематика рефератов и др., список рекомендуемой литературы, информационных ресурсов и др.).

Темы для устного опроса:

1. Обзор средств информационной безопасности в различных ОС (не рассматриваемых в рамках учебной дисциплины)
2. Обзор недавно найденных уязвимостей в операционных системах
3. Обзор уязвимостей в сетевых протоколах

Примерный перечень вопросов к зачету

1. Оценка рисков информационной безопасности
2. Безопасное программирование
3. Информационная безопасность в ОС Windows
4. Механизм User Account Control в ОС Windows
5. Информационная безопасность в ОС macOS
6. Информационная безопасность в ОС Linux
7. Информационная безопасности в ОС iOS
8. Информационная безопасности в ОС iOS
9. Инструменты анализа уязвимостей
10. Инструменты анализа кода

Примерный перечень вопросов к экзамену

1. Стандарты информационной безопасности
2. Оценка рисков информационной безопасности
3. Безопасное программирование
4. Стандарты MISRA и HIC++
5. Инструменты анализа кода
6. Контроль и аудит доступа в ОС Windows

7. Привилегии, токены, имперсонация
8. Механизм User Account Control
9. Подсистема WSL
10. Системные программы в Windows
11. Контроль и аудит доступа в ОС Linux
12. Команда sudo
13. Информационная безопасность в macOS
14. Парольные политики в Linux
15. Архитектура ОС Android
16. Разрешения в Android
17. Архитектура ОС iOS
18. Разрешения в iOS
19. Особенности ОС на встраиваемых и носимых устройствах
20. Инструменты сбора информации
21. Инструменты анализа локальных уязвимостей
22. Инструменты анализа трафика и сетевых уязвимостей
23. Фреймворк Metasploit
24. Противодействие обходу механизмов безопасности

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УВО

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Методы машинного обучения в информационной безопасности	Технологий программирования	Нет	Оставить содержание учебной дисциплины без изменения, протокол № 16 от 28.05.2021

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ

на _____/_____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры
_____ (протокол № ____ от _____ 20__ г.)

Заведующий кафедрой
_____ _____ _____

УТВЕРЖДАЮ
Декан факультета
_____ _____ _____