Учреждение образования
«Полоцкий государственный университет имени Евфросинии Полоцкой»

УТВЕРЖДАЮ
Ректор учреждения образования
«Полоцкий государственный
университет имени
Евфросинии Полоцкой»
_____ Ю.Я. Романовский
«17» 06 2025 г.
Регистрационный №УД-1109-25/уч

ЗАЩИТА ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Учебная программа учреждения образования
по учебной дисциплине для специальности
6-05-0533-12 «Кибербезопасность»

2025 г.

Учебная программа составлена на основе образовательного стандарта по специальности высшего образования ОСВО 6-05-0533-12-2023 и учебного плана специальности 6-05-0533-12 «Кибербезопасность». Регистрационный 14-23/уч. ФКНЭ от 04.04.2023 для дневной формы получения высшего образования

СОСТАВИТЕЛЬ:

Сергей Васильевич Кухта, старший преподаватель кафедры математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой» (протокол № 6 от «30» мая 2025 г.)

Научно-методическим советом учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой» (протокол № 7 от «27» июня 2025 г.)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Особую сложность, наряду с поиском, локализацией и устранением программных ошибок, представляет собой обнаружение вредоносных программ, преднамеренно вносимых в программное обеспечение (ПО) как на этапе создания программных комплексов, так и на этапе их эксплуатации. Кроме того, существенный урон производителю программных продуктов наносят такие неавторизованные действия, как несанкционированное исследование, копирование программ, их незаконное распространение и использование. Это наносит значительный моральный и материальный ущерб фирмам-изготовителям программного обеспечения, а часто и легитимным потребителям программного продукта.

Дисциплина «Защита от вредоносного программного обеспечения» предназначена для обучения студентов основам защиты программного обеспечения и операционных систем (ОС) от воздействий вредоносного программного обеспечения.

В учебной дисциплине «Защита от вредоносного программного обеспечения» рассмотрены элементы методологии защиты ПО, описаны уязвимости и угрозы ПО и принципы обеспечения его безопасности. Изучаются методы защиты ПО от вредоносных программ, методы обеспечения технологической безопасности программ, реализуемые на этапах тестирования и испытания программных комплексов, некоторые вопросы, связанные с защитой операционных систем. Также представлены современные средства, системы и комплексы защиты ПО на этапе эксплуатации: средства тестирования и обфускации программ, защите программ от несанкционированного копирования. Наряду с научно-практическими мероприятиями по защите современного ПО в учебной дисциплине рассматриваются организационно-технические и нормативно-правовые аспекты разработки и эксплуатации программ, в том числе процесс сертификации программных комплексов по требованиям безопасности информации.

Цель изучения учебной дисциплины «Защита от вредоносного программного обеспечения»: овладение теоретическими знаниями и формирование практических умений и навыков в области обеспечения безопасности ПО, в том числе освоение комплекса мер, методов и способов защиты программ от различного рода деструктивных угроз в процессе их возникновения и реализации в современных информационных системах.

Задачи, решаемые при изучении учебной дисциплины «Защита от вредоносного программного обеспечения»:

– изучение современных тенденций развития вредоносных программ и современных средств и методов борьбы с ними;

– изучение программирования средств антивирусной защиты информации;

– приобретение навыков программирования антивирусных средств защиты в средах Windows, Linux и Android;

– изучение организации процесса разработки антивирусного программного обеспечения;

– изучение организации защиты информационных систем от вредоносного ПО.

При изучении дисциплины «Защита от вредоносного программного обеспечения» у студентов специальности 6-05-0533-12 «Кибербезопасность» должен сформироваться набор компетенций, соответствующих присваиваемой по завершению высшего образования квалификации «Специалист по кибербезопасности», обеспечивающих выпускникам успешность применения полученных знаний и умений в дальнейшей профессиональной деятельности:

специализированные компетенции:

- Разрабатывать программное обеспечение в интегрированных средах разработки. Использовать автоматизированные средства разработки программных средств. Разрабатывать необходимую для этого документацию.

- Владеть методами построения надежных блочных и поточных криптосистем, функций хеширования, криптосистем с открытым ключом и систем электронной цифровой подписи.

универсальные компетенции:

- Владеть основами исследовательской деятельности, осуществлять поиск, анализ и синтез информации.
- Решать стандартные задачи профессиональной деятельности на основе применения информационно-коммуникационных технологий.
- Быть способным к саморазвитию и совершенствованию в профессиональной деятельности.
- Проявлять инициативу и адаптироваться к изменениям в профессиональной деятельности.

В результате освоения учебной дисциплины студент должен:

знать:

– наиболее распространенные в настоящее время типы вредоносных программ;

– особенности современных вредоносных программ;

– существующие методы и средства борьбы с вредоносными программами;

– основные проектные решения, средства и методы защиты информации от несанкционированного доступа;

– средства организации процесса разработки антивирусного программного обеспечения;

– методы испытания антивирусных программных средств;

уметь:

– применять полученные знания для создания надежных систем защиты информации;

– решать типовые задачи с помощью методов защиты информации от несанкционированного доступа;

– применять существующие методы защиты информации от несанкционированного доступа без снижения их стойкости за счет принятия неправильных эксплуатационных решений;

– применять современные методы и методики защиты программ от программных средств скрытого информационного воздействия;

– применять современные методы и методики защиты программ от несанкционированного исследования, копирования, распространения и использования;

владеть:

– методами разработки и использования защищенных программных средств;

– навыками эксплуатации защищенных программных средств, получивших широкое применение в современных автоматизированных системах;

– правовыми и организационными методами защиты информации в информационной системе.

Связи с другими учебными дисциплинами

Основой для изучения учебной дисциплины «Защита от вредоносного программного обеспечения» по специальности 6-05-0533-12 «Кибербезопасность» являются учебные дисциплины «Программирование на C++», «Основы кибербезопасности», «Криптографические методы защиты информации».

Знания, полученные при изучении учебной дисциплины «Защита от вредоносного программного обеспечения», являются основой для дипломного проектирования, используются учебными дисциплинами «Программно-аппаратные и технические средства защиты информации», «Криптографический инжиниринг», «Методы и стандарты оценки защищенности компьютерных систем».

Форма получения высшего образования – дневная.

В соответствии с учебным планом по специальности 6-05-0533-12 «Кибербезопасность» на изучение учебной дисциплины отводится:

Форма получения высшего образования	дневная
Курс (курсы)	3
Семестр	5
Всего часов по дисциплине	108
Всего аудиторных часов по дисциплине	66
В том числе:	
Лекций, часов	32
Лабораторные занятия, часов	34
Самостоятельная работа, часов	42
Форма промежуточной аттестации	зачет
Трудоемкость дисциплины, зачетные единицы	3
Курсовой проект, часов	40
Трудоемкость курсового проекта, зачетные единицы	1

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1. МЕТОДЫ ОБЕСПЕЧЕНИЯ ТЕХНОЛОГИЧЕСКОЙ И ЭКСПЛУАТАЦИОННОЙ БЕЗОПАСНОСТИ ПО

Тема 1.1. Введение в теорию и практику защиты ПО.

Проблема защиты ПО ИС. Объекты защиты. Уязвимости и угрозы безопасности ПО. Несанкционированные исследование и копирование программ. Жизненный цикл ПО информационных систем. Технологическая и эксплуатационная безопасность ПО. Основные принципы обеспечения безопасности ПО. Защита ПО как система научных дисциплин.

Тема 1.2. Классификация вредоносных программ.

Принципы классификации вредоносных программ. Троянские программы. Компьютерные вирусы. Прочие вредоносные программ. Особенности вредоносных программ нового поколения. Средства доставки вредоносных программ до объектов их атаки. Защита от вредоносных программ.

Тема 1.3. Методы тестирования ПО на его защищенность.

Методы тестирования программ. Фаззинг программ.

Тема 1.4. Методы защиты программ от несанкционированного исследования.

Классификация средств несанкционированного исследования программ. Способы защиты программ от несанкционированного исследования. Обфускация программ. Способы встраивания защитных механизмов в ПО.

Тема 1.5. Методы защиты программ от несанкционированного копирования.

Криптографические методы защиты от копирования. Метод привязки к идентификатору. Методы, основанные на работе с переходами и стеком. Манипуляции с кодом программы. Методы противодействия динамическим способам снятия защиты программ от копирования.

Тема 1.6. Методы описания и обнаружения уязвимостей ПО на примере операционных систем.

Уязвимости на примере операционной системы Windows. Методы обнаружения уязвимостей операционных систем. Подходы к разработке защищенных операционных систем.

Раздел 2. СРЕДСТВА, СИСТЕМЫ И КОМПЛЕКСЫ ЗАЩИТЫ ПО

Тема 2.1. Средства, системы и комплексы тестирования ПО при испытаниях его на технологическую безопасность.

Средства и комплексы защиты от вредоносных программ. Методологические основы оценки качества, проведения испытаний и сертификации программных средств. Построение программно-аппаратных комплексов для контроля технологической безопасности программ. Фаззеры программ. Пример тестирования ПО средств защиты информации.

Тема 2.2. Обфускаторы программ.

Задача и цели и обфускации. Оценка эффективности обфускации. Примеры обфускаторов программ, написанных на скриптовых языках.

Тема 2.3. Способы и средства защиты программ от несанкционированного копирования.

Уязвимости методов защиты ПО от копирования. Проверка оригинального носителя. Ввод серийного номера. Активация ПО. Использование электронных ключей. Использование автоматических средств защиты.

Тема 2.4. Защищенные операционные системы.

Создание дистрибутива ОС Linux с повышенными требованиями к ее защищенности.

Пример построения мобильной защищенной операционной системы на базе Android.

Раздел 3. ИССЛЕДОВАНИЕ ПО НА ПРЕДМЕТ ОТСУТСТВИЯ НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ

Тема 3.1. Сертификация средств защиты информации по требованиям безопасности информации.

Проверка соответствия реальных и декларируемых функциональных возможностей. Проверка отсутствия недекларируемых возможностей. Методы проведения испытаний. Документация, представляемая на испытания.

Тема 3.2. Статический анализ исходных текстов и исполняемых модулей ПО.

Контроль полноты и отсутствия избыточности исходных текстов на уровне файлов. Контроль соответствия исходных текстов ПО его объектному коду. Контроль связей функциональных объектов по управлению и информации. Синтаксический контроль наличия заданных конструкций. Формирование и анализ маршрутов выполнения функциональных объектов. Динамический анализ исходных текстов программ.

ТРЕБОВАНИЯ К КУРСОВОМУ ПРОЕКТУ

Курсовой проект по дисциплине «Защита от вредоносного программного обеспечения» - работа студента, предназначенная для объективного контроля: степени освоения знаний, полученных студентами при изучении теоретического материала дисциплины; умений и навыков, полученных при выполнении лабораторных работ; применения знаний, умений и навыков к решению конкретных инженерных задач защиты программного обеспечения; развитие навыков инженерного проектирования и навыков работы со специальной литературой, предусматривающих проведение анализа и согласно требованиям задания на курсовое проектирование.

Целью курсового проекта является:

- систематизация знаний и накопление практического опыта в области проектирования и реализации систем обеспечения безопасности ПО, в том числе освоение комплекса мер, методов и способов защиты программ от различного рода деструктивных угроз в процессе их возникновения и реализации в современных информационных системах;
- формирование навыков самостоятельной работы по решению проблем защиты программного обеспечения.

В состав курсового проекта входят:

- пояснительная записка;
- графическая часть;
- работающее программное средство.

Пояснительная записка должна отражать основные этапы разработки курсового проекта. Графическая часть представляет собой диаграммы в нотации UML, показывающие основные алгоритмы, реализованные в курсовом проекте. Программное средство может разрабатываться на любом языке программирования.

На выполнение курсового проекта отводится 40 часов.

Перечень тем курсовых проектов

1. Антивирусный комплекс для защиты рабочих станций
2. Антивирусный комплекс для защиты сетевых серверов
3. Антивирусный комплекс для защиты почтовых систем
4. Антивирусный комплекс для защиты шлюзов
5. Антивирусный комплекс для хостов (домашних персональных компьютеров)
6. Антивирусный комплекс для мобильных устройств
7. Методы обнаружения и устранения вредоносного ПО в Windows-подобных операционных системах
8. Методы обнаружения и устранения вредоносного ПО в Linux-подобных операционных системах
9. Методы обнаружения и устранения вредоносного ПО в операционных системах для мобильных устройств
10. Оценка эффективности систем защиты программного обеспечения
11. Анализ средств преодоления систем защиты программного обеспечения
12. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов
13. Обзор и анализ современных программно-аппаратных средств защиты информации
14. Выбор оптимального средства защиты информации исходя из имеющихся исходных данных
15. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии
16. Проблема защиты информации в облачных хранилищах данных и центрах обработки данных

17. Защита сред виртуализации
18. Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах
19. Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности
20. Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности
21. Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов
22. Диагностика и оценка качества антивирусной программы
23. Разработка сетевой политики защиты от вредоносных программ
24. Подбор и анализ программного обеспечения для защиты от вредоносных программ в сети
25. Установка комплексной защиты от вредоносных программ
26. Тестирование системы защиты программного обеспечения
27. Испытания программных средств на наличие вредоносного ПО
28. Статический анализ исходного кода
29. Динамический анализ исходного кода
30. Аттестация программного обеспечения на отсутствие недекларированных возможностей.

Учебно-методическая карта учебной дисциплины «Защита от вредоносного программного обеспечения»
Дневная форма получения высшего образования

Номер раздела, темы	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов				Литература	Формы контроля знаний
		Лекции	Лабораторные занятия	Практические занятия	Управляемая самостоятельная работа студента		
1	2	3	4	5	6	7	8
Раздел 1	**Методы обеспечения технологической и эксплуатационной безопасности ПО**	**18**	**22**				
Тема 1.1	***Введение в теорию и практику защиты программного обеспечения.*** Проблема защиты ПО ИС. Объекты защиты. Уязвимости и угрозы безопасности программного обеспечения. Классификация вредоносных программ. Несанкционированные исследование и копирование программ.	2				Осн. лит.: [1], [2]. Доп. лит.: [2]. Стандарты: [1].	Блиц-опрос
	Жизненный цикл ПО информационных систем. Технологическая и эксплуатационная безопасность ПО. Основные принципы обеспечения безопасности ПО. Защита ПО как система научных дисциплин.	2					
Тема 1.2	***Классификация вредоносных программ.*** Принципы классификации вредоносных программ. Троянские программы. Компьютерные вирусы. Прочие вредоносные программ.	2				Осн. лит.: [1], [2]. Доп. лит.: [2]. Стандарты: [1], [3], [4].	Блиц-опрос
	Особенности вредоносных программ нового поколения. Средства доставки вредоносных программ до объектов их атаки. Защита от вредоносных программ.	2					
	Лабораторная работа №1. Защита от компьютерных вирусов.		2			Методические указания	Защита отчета по лабораторной работе
	Лабораторная работа №2. Разработка и обнаружение вредоносной программы деструктивного типа.		2			Методические указания	Защита отчета по лабораторной работе

1	2	3	4	5	6	7	8
	Лабораторная работа №2. Разработка и обнаружение вредоносной программы деструктивного типа.		2				
Тема 1.3	***Методы тестирования ПО на его защищенность.*** Методы тестирования программ. Фаззинг программ.	2				Осн. лит.: [1], [2]. Доп. лит.: [2].	Блиц-опрос
	Лабораторная работа №3. Фаззинг программ.		2			Методические указания	Защита отчета по лабораторной работе
Тема 1.4	***Методы защиты программ от несанкционированного исследования.*** Классификация средств несанкционированного исследования программ. Способы защиты программ от несанкционированного исследования. Обфускация программ. Способы встраивания защитных механизмов в ПО.	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [2], [3]. Стандарты: [2].	Контрольное тестирование №1
	Лабораторная работа №4. Встраивание защитных механизмов в ПО.		2			Методические указания	Защита отчета по лабораторной работе
	Лабораторная работа №4. Встраивание защитных механизмов в ПО.		2				
Тема 1.5	***Методы защиты программ от несанкционированного копирования.*** Криптографические методы защиты от копирования. Метод привязки к идентификатору. Методы, основанные на работе с переходами и стеком.	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [2], [3]. Стандарты: [2].	Блиц-опрос
	Манипуляции с кодом программы. Методы противодействия динамическим способам снятия защиты программ от копирования.	2					
	Лабораторная работа №5. Защита программы от несанкционированного копирования привязкой к конфигурации вычислительной системы.		2			Методические указания	Защита отчета по лабораторной работе
	Лабораторная работа №5. Защита программы от несанкционированного копирования привязкой к конфигурации вычислительной системы.		2				
Тема 1.6	***Методы описания и обнаружения уязвимостей ПО на примере операционных систем.*** Уязвимости на примере операционной системы Windows. Методы обнаружения уязвимостей операционных систем. Подходы к разработке защищенных операционных систем.	2				Осн. лит.: [1], [2]. Доп. лит.: [2]. Стандарты: [2], [4].	Блиц-опрос
	Лабораторная работа №6. Исследование уязвимостей операционных систем.		2			Методические указания	Защита отчета по лабораторной работе

1	2	3	4	5	6	7	8
	Лабораторная работа №7. Разработка программы фильтрации сетевых пакетов по нескольким критериям.		2			Методические указания	Защита отчета по лабораторной работе
Раздел 2	**Средства, системы и комплексы защиты ПО.**	**8**	**10**				
Тема 2.1	***Средства, системы и комплексы тестирования ПО при испытаниях его на технологическую безопасность.*** Средства и комплексы защиты от вредоносных программ. Методологические основы оценки качества, проведения испытаний и сертификации программных средств. Построение программно-аппаратных комплексов для контроля технологической безопасности программ. Фаззеры программ. Пример тестирования ПО средств защиты информации.	2				Осн. лит.: [1], [2]. Доп. лит.: [2]. Стандарты: [2].	Контрольное тестирование №2
	Лабораторная работа №8. Разработка и обнаружение вредоносной программы , обеспечивающей утечку конфиденциальной информации.		2			Методические указания	Защита отчета по лабораторной работе
	Лабораторная работа №8. Разработка и обнаружение вредоносной программы, обеспечивающей утечку конфиденциальной информации.		2				
Тема 2.2	***Обфускаторы программ.*** Задача и цели и обфускации. Оценка эффективности обфускации. Примеры обфускаторов программ, написанных на скриптовых языках.	2				Осн. лит.: [1], [2]. Доп. лит.: [1], [2].	Блиц-опрос
Тема 2.3	***Способы и средства защиты программ от несанкционированного копирования.*** Уязвимости методов защиты ПО от копирования. Проверка оригинального носителя. Ввод серийного номера. Активация ПО. Использование электронных ключей. Использование автоматических средств защиты.	2				Осн. лит.: [1], [2]. Доп. лит.: [1], [2].	Блиц-опрос
	Лабораторная работа №9. Реализация алгоритмов защиты программы от несанкционированной эксплуатации.		2			Методические указания	Защита отчета по лабораторной работе
	Лабораторная работа №9. Реализация алгоритмов защиты программы от несанкционированной эксплуатации.		2				

1	2	3	4	5	6	7	8
Тема 2.4	***Защищенные операционные системы.*** Создание дистрибутива ОС Linux с повышенными требованиями к ее защищенности. Пример построения мобильной защищенной операционной системы на базе Android.	2				Осн. лит.: [1], [2]. Доп. лит.: [1], [2].	Блиц-опрос
	Лабораторная работа №10. Разработка программы, обнаруживающей атаку типа ARP-poisoning.		2			Методические указания	Защита отчета по лабораторной работе
Раздел 3	**Исследование ПО на предмет отсутствия недекларированных возможностей.**	**6**	**4**				
Тема 3.1	***Сертификация средств защиты информации по требованиям безопасности информации.*** Проверка соответствия реальных и декларируемых функциональных возможностей. Проверка отсутствия недекларируемых возможностей. Методы проведения испытаний. Документация, представляемая на испытания.	2				Осн. лит.: [1]. Доп. лит.: [2]. Стандарты: [2].	Блиц-опрос
	Лабораторная работа №10. Разработка программы, обеспечивающей обнаружение вредоносного кода по сигнатурам, взятым из заранее заданного файла.		2			Методические указания	Защита отчета по лабораторной работе
Тема 3.2	***Статический анализ исходных текстов и исполняемых модулей ПО.*** Контроль полноты и отсутствия избыточности исходных текстов на уровне файлов. Контроль соответствия исходных текстов ПО его объектному коду. Контроль связей функциональных объектов по управлению и информации.	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [1], [2].	Контрольное тестирование №3
	Синтаксический контроль наличия заданных конструкций. Формирование и анализ маршрутов выполнения функциональных объектов. Динамический анализ исходных текстов программ.	2					
	Лабораторная работа №11. Статический анализ исходных текстов и исполняемых модулей ПО.		2			Методические указания	Защита отчета по лабораторной работе
	Всего (66 часов)	**32**	**34**				

Примечание: в соответствии с рейтинговой системой для определения результата текущего контроля за семестр в виде отметки в баллах по десятибалльной шкале используются отметки, полученные за мероприятия текущего контроля в течение семестра, обозначенные в графе «Форма контроля знаний»

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ЛИТЕРАТУРА

Основная:

1. Баланов, А. Н. Защита информационных систем. Кибербезопасность : учебное пособие для вузов / А. Н. Баланов. – 2-е изд., стер. – Санкт-Петербург : Лань, 2025. — 280 с. – ISBN 978-5-507-50467-1. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/438971 (дата обращения: 30.09.2025). – Режим доступа: для авториз. пользователей.

2. Фот, Ю. Д. Анализ уязвимостей и защита программного обеспечения: практикум : учебное пособие / Ю. Д. Фот, Е. И. Ларионова. – Оренбург : ОГУ, 2025. – 141 с. – ISBN 978-5-7410-3391-3. – Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/502991 (дата обращения: 30.09.2025). – Режим доступа: для авториз. пользователей.

3. Фомичев, В.М. Криптографические методы защиты информации: учебник для вузов: в 2 частях. Часть 2 : Системные и прикладные аспекты. / В. М. Фомичев, Д. А. Мельников ; под редакцией В.М. Фомичева. - Москва: Юрайт, 2023. – 245 с.

Дополнительная:

1. Платонов, В. В. Технологии машинного обучения в кибербезопасности : учебное пособие / В. В. Платонов. - Москва ; Вологда : Инфра-Инженерия, 2024. – 140 с. – ISBN 978-5-9729-2048-8. – Текст : электронный. – URL: https://znanium.ru/catalog/product/2170891 (дата обращения: 30.09.2025). – Режим доступа: по подписке.

2. Прохорова, О. В. Информационная безопасность и защита информации: учебник / О. В. Прохорова. – 2-е изд., испр. – Санкт-Петербург : Лань, 2020. – 124 с. – ISBN 978-5-8114-4404-5. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/133924 (дата обращения: 19.08.2022). – Режим доступа: для авториз. пользователей.

3. Алгоритмы шифрования. Специальный справочник / С. П. Панасенко. – СПб.: БХВ-Петербург, 2009. – 577 с. – Текст : электронный.

Стандарты, действующие в Республике Беларусь:

1. СТБ 34.101.8-2006 «Информационные технологии. Методы и средства безопасности. Программные и программно-аппаратные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования»

2. ГОСТ ISO/IEC TS 19249-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Каталог принципов построения архитектуры и проектирования безопасных продуктов, систем и приложений»

3. СТБ 34.101.75-2017 «Информационные технологии. Системы обнаружения и предотвращения вторжений. Общие требования».

4. СТБ 34.101.76-2017 «Информационные технологии. Методы и средства безопасности. Системы обнаружения и предотвращения утечек информации из информационных систем. Общие требования».

Гурова Е. В.

ПЕРЕЧЕНЬ ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Лабораторная работа №1 Защита от компьютерных вирусов.

Лабораторная работа №2 Разработка и обнаружение вредоносной программы деструктивного типа.

Лабораторная работа №3 Фаззинг программ.

Лабораторная работа №4 Встраивание защитных механизмов в ПО.

Лабораторная работа №5 Защита программы от несанкционированного копирования привязкой к конфигурации вычислительной системы.

Лабораторная работа №6 Исследование уязвимостей операционных систем.

Лабораторная работа №7 Разработка программы фильтрации сетевых пакетов по нескольким критериям.

Лабораторная работа №8 Разработка и обнаружение вредоносной программы, обеспечивающей утечку конфиденциальной информации.

Лабораторная работа №9 Реализация алгоритмов защиты программы от несанкционированной эксплуатации.

Лабораторная работа №10 Разработка программы, обеспечивающей обнаружение вредоносного кода по сигнатурам, взятым из заранее заданного файла.

Лабораторная работа №11 Статический анализ исходных текстов и исполняемых модулей ПО.

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ЗАЧЕТА

1. Проблема защиты ПО ИС. Объекты защиты.
2. Уязвимости и угрозы безопасности ПО.
3. Несанкционированные исследование и копирование программ.
4. Технологическая и эксплуатационная безопасность ПО.
5. Основные принципы обеспечения безопасности ПО.
6. Защита ПО как система научных дисциплин.
7. Классификация вредоносных программ.
8. Троянские программы.
9. Компьютерные вирусы.
10. Прочие вредоносные программ.
11. Особенности вредоносных программ нового поколения.
12. Средства доставки вредоносных программ до объектов их атаки.
13. Защита от вредоносных программ.
14. Методы тестирования ПО на его защищенность.
15. Фаззинг программ.
16. Классификация средств несанкционированного исследования программ.
17. Способы защиты программ от несанкционированного исследования.
18. Обфускация программ.
19. Способы встраивания защитных механизмов в ПО.
20. Криптографические методы защиты от копирования.
21. Метод привязки к идентификатору.
22. Методы, основанные на работе с переходами и стеком.
23. Манипуляции с кодом программы.
24. Методы противодействия динамическим способам снятия защиты программ от копирования.
25. Уязвимости на примере операционной системы Windows.
26. Методы обнаружения уязвимостей операционных систем.
27. Подходы к разработке защищенных операционных систем.
28. Методологические основы оценки качества, проведения испытаний и сертификации программных средств.
29. Построение программно-аппаратных комплексов для контроля технологической безопасности программ.
30. Фаззеры программ.
31. Задача и цели и обфускации.
32. Оценка эффективности обфускации.
33. Уязвимости методов защиты ПО от копирования.
34. Проверка оригинального носителя.
35. Ввод серийного номера.
36. Использование электронных ключей.
37. Использование автоматических средств защиты.
38. Создание дистрибутива ОС Linux с повышенными требованиями к ее защищенности.
39. Сертификация средств защиты информации по требованиям безопасности информации.
40. Проверка соответствия реальных и декларируемых функциональных возможностей.
41. Проверка отсутствия недекларируемых возможностей.
42. Методы проведения испытаний.
43. Документация, представляемая на испытания.
44. Контроль полноты и отсутствия избыточности исходных текстов на уровне файлов.
45. Контроль соответствия исходных текстов ПО его объектному коду.
46. Контроль связей функциональных объектов по управлению и информации.
47. Синтаксический контроль наличия заданных конструкций.
48. Формирование и анализ маршрутов выполнения функциональных объектов.
49. Динамический анализ исходных текстов программ.

ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Обучение дисциплине «Защита от вредоносного программного обеспечения» предполагает реализацию следующих форм самостоятельной работы студентов:

– проработка конспекта лекций и учебной литературы;

– изучение печатных источников по теме дисциплины;

– изучение профессиональных электронных ресурсов по теме дисциплины;

– изучение вопросов для самоконтроля;

– подготовка к аудиторному выполнению лабораторных работ (предварительное знакомство с методическими указаниями, вариантом индивидуального задания по работе);

– решение индивидуальных задач при подготовке к лабораторным занятиям;

–подготовка к защите лабораторных работ (оформление отчёта по индивидуальному варианту задания, защита результатов работы и демонстрации степени освоения навыков и умений по конкретной теме);

–углублённое изучение отдельных тем учебной дисциплины для подготовки к устным опросам;

– изучение основной и дополнительной литературы в процессе подготовки к анализу и решению проблемных задач, реализации элементов исследовательской деятельности;

–систематизация полученных знаний при подготовке к зачету.

Условия для самостоятельной работы студентов, в частности, для развития навыков самоконтроля, способствующих интенсификации образовательного процесса, обеспечиваются:

– наличием и использованием в образовательном процессе учебного курса по дисциплине «Защита от вредоносного программного обеспечения» в системе дистанционного обучения Moodle для доступа студентов к электронным вариантам курса лекций и учебно-методических указаний по основным разделам дисциплины, для организации учебной деятельности студентов и контроля ее результативности.

Дополнительное учебно-методическое обеспечение самостоятельной работы студентов очной формы обучения

1. Учебный курс по дисциплине «Защита от вредоносного программного обеспечения» в системе дистанционного обучения Moodle (ссылка https://moodle.psu.by/course/view.php?id=268).

2. Методические указания к выполнению лабораторных работ по дисциплине «Защита от вредоносного программного обеспечения» для студентов специальности 6-05-0533-12 «Кибербезопасность»

Содержание самостоятельной работы студентов дневной формы получения высшего образования

Вид самостоятельной работы	Тематическое содержание и используемые источники	Количество часов
1	2	3
Самостоятельное изучение отдельных вопросов по темам дисциплины	*Тема 1.4. Методы защиты программ от несанкционированного исследования.* Способы защиты программ от несанкционированного исследования. Обфускация программ. Способы встраивания защитных механизмов в ПО Осн. лит.: [1], [2], [3]. Доп. лит.: [2], [3].	2
	Тема 1.5. Методы защиты программ от несанкционированного копирования. Криптографические методы защиты от копирования. Метод привязки к идентификатору. Методы, основанные на работе с переходами и стеком. Манипуляции с кодом программы. Методы противодействия динамическим способам снятия защиты программ от копирования. Осн. лит.: [1], [2], [3]. Доп. лит.: [2], [3].	3
	Тема 2.1. Средства, системы и комплексы тестирования ПО при испытаниях его на технологическую безопасность. Средства и комплексы защиты от вредоносных программ. Методологические основы оценки качества, проведения испытаний и сертификации программных средств. Построение программно-аппаратных комплексов для контроля технологической безопасности программ. Фаззеры программ. Пример тестирования ПО средств защиты информации. Осн. лит.: [1], [2]. Доп. лит.: [2].	2
	Тема 2.3. Способы и средства защиты программ от несанкционированного копирования. Уязвимости методов защиты ПО от копирования. Проверка оригинального носителя. Ввод серийного номера. Активация ПО. Использование электронных ключей. Использование автоматических средств защиты. Осн. лит.: [1], [2]. Доп. лит.: [1], [2].	3
	Тема 3.2. Статический анализ исходных текстов и исполняемых модулей ПО. Контроль полноты и отсутствия избыточности исходных текстов на уровне файлов. Контроль соответствия исходных текстов ПО его объектному коду. Контроль связей функциональных объектов по управлению и информации. Синтаксический контроль наличия заданных конструкций. Формирование и анализ маршрутов выполнения функциональных объектов. Динамический анализ исходных текстов программ. Осн. лит.: [1], [2], [3]. Доп. лит.: [1], [2].	3
Подготовка к защите отчетов по лабораторным работам	*Лабораторная работа №1* Защита от компьютерных вирусов.	2
	Лабораторная работа № 2 Разработка и обнаружение вредоносной программы деструктивного типа.	3
	Лабораторная работа №3 Фаззинг программ.	3
	Лабораторная работа №4 Встраивание защитных механизмов в ПО.	3

1	2	3
	Лабораторная работа №5 Защита программы от несанкционированного копирования привязкой к конфигурации вычислительной системы.	3
	Лабораторная работа №6 Исследование уязвимостей операционных систем.	2
	Лабораторная работа №7 Разработка программы фильтрации сетевых пакетов по нескольким критериям.	2
	Лабораторная работа №8 Разработка и обнаружение вредоносной программы, обеспечивающей утечку конфиденциальной информации.	3
	Лабораторная работа №9 Реализация алгоритмов защиты программы от несанкционированной эксплуатации.	3
	Лабораторная работа №10 Разработка программы, обеспечивающей обнаружение вредоносного кода по сигнатурам, взятым из заранее заданного файла.	2
	Лабораторная работа №11 Статический анализ исходных текстов и исполняемых модулей ПО.	3
		42

КОНТРОЛЬ КАЧЕСТВА УСВОЕНИЯ ЗНАНИЙ

Контроль качества усвоения знаний проводится в форме текущего контроля и промежуточной аттестации.

Мероприятия текущего контроля проводятся в течение семестра и включают в себя следующие **формы контроля:**

–устная форма (блиц-опрос на лекциях);

–письменная форма (тесты, письменные отчёты по лабораторным работам);

–устно-письменная форма (отчёты по лабораторным работам с их устной защитой);

–техническая форма (электронные тесты).

Лабораторные работы предполагают выполнение и защиту. При их выполнении выдаётся индивидуальное задание. Отчёт по лабораторной работе представляется в электронном виде. Содержание отчёта: название работы, вариант задания, анализ задания, ход выполнения работы, основные и промежуточные результаты, выводы по работе. Защита работ проводится индивидуально и оценивается в соответствии с установленными правилами.

Результат текущего *контроля за семестр* оценивается отметкой в баллах по десятибалльной шкале и выводится исходя из отметок, выставленных в ходе проведения мероприятий текущего контроля в течение семестра по следующей формуле:

$$\text{Т} = \frac{(\text{КТ}_1 + \ldots + \text{КТ}_{n1}) + (\text{ЛР}_1 + \cdots + \text{ЛР}_{n2}) + (\text{УО}_1 + \cdots + \text{УО}_{n3})}{(n1 + n2 + n3)},$$

где $\text{КТ}_1, \ldots, \text{КТ}_{n1}$ – отметки, выставленные по результатам контрольного тестирования; $n1$ – количество тестов; $\text{ЛР}_1, \ldots, \text{ЛР}_{n2}$ – отметки, выставленные по результатам защит лабораторных работ; $n2$ – количество работ; УО_1, ..., УО_{n3} – отметки, выставленные по результатам устных опросов на лекциях; $n3$ – количество устных опросов.

Результат текущего контроля рассчитывается как округлённое среднее значение.

Для обучающего, пропустившего мероприятие текущего контроля по уважительной причине, кафедрой устанавливаются дополнительные сроки.

Обучающемуся, пропустившему мероприятие текущего контроля без уважительной причины, выставляется 1 (один) балл за данное мероприятие.

Результат текущего контроля может быть повышен:

- за участие обучающего в научно-практических мероприятиях, учебно-исследовательской, научно-исследовательской работе студентов (конференциях, семинарах, олимпиадах, конкурсах, научных кружках и т.п.) по профилю учебной дисциплины (модуля) и может быть повышен до 10 баллов при достижении значимых результатов в этой работе;

- обучающийся в целях повышения отметки по любому мероприятию текущего контроля может воспользоваться правом на дополнительные образовательные услуги (платные консультации, платные дополнительные занятия). Количество и сроки пересдач с целью повышения отметки определяет кафедра.

Промежуточная аттестация проводится в форме зачёта в пятом семестре.

Заключение о *зачёте* формируется по формуле:

$$З = k \cdot \text{Т},$$

где k – весовой коэффициент текущего контроля; Т – результат текущего контроля за семестр. Весовой коэффициент k принимается равным 1.

Если полученная отметка $З < 4$ баллов, то проводится устный зачёт отдельно по представленным в программе вопросам.

Перевод отметки по зачету осуществляется по следующим правилам: отметка «зачтено» выставляется студентам, получившим от 4 до 10 баллов, отметка «не зачтено» выставляется студентам, получившим от 1 до 3 баллов.

ХАРАКТЕРИСТИКА ИННОВАЦИОННЫХ ПОДХОДОВ К ПРЕПОДАВАНИЮ УЧЕБНОЙ ДИСЦИПЛИНЫ

Основные методы (технологии) обучения, отвечающие целям и задачам учебной дисциплины:

– проблемное обучение (проблемное изложение, вариативное изложение), реализуемое на лекционных занятиях;

– учебно-исследовательская деятельность, реализация творческого подхода, реализуемые на лабораторных занятиях.

Используемые технологии обучения и диагностики компетенций в преподавании дисциплины «Защита от вредоносного программного обеспечения» реализуют подход, основанный на максимально возможном использовании внутренней и учебной мотивации студента, проявляющейся в чётком понимании им значимости всех видов выполняемых работ, как с точки зрения важности для профессиональной подготовки, так и с точки зрения оценивания. Подход предполагает использование элементов проблемного обучения и элементов исследовательской деятельности студентов в процессе аудиторной работы, а также при выполнении самостоятельных работ при постоянном рейтинговом контроле.

На лекционных занятиях по дисциплине «Защита от вредоносного программного обеспечения» возможно использование элементов проблемного обучения: проблемное изложение некоторых аспектов, использование частично-поискового метода.

Изучение учебной дисциплины осуществляется на лекционных и лабораторных занятиях.

На лекционных занятиях студенты овладевают системой теоретических знаний в области методов криптографической защиты информации. В ходе лекционного изложения теоретических сведений используются традиционные словесные приёмы и методы, которые активизируются постановкой проблемных вопросов и заданий, организацией учебных дискуссий с опорой на имеющуюся начальную подготовку студентов и их математический кругозор, использованием интерактивных методов обучения.

На лабораторных занятиях развиваются и формируются необходимые практические умения и навыки программной реализации криптографических методов защиты информации.

Применяется индивидуальный, творческий подход. Также во время проведения лабораторных работ особое внимание уделяется формированию у студентов умения планировать свою работу и определять эффективную последовательность её выполнения.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ С ДРУГИМИ УЧЕБНЫМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Название 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
Дипломное проектирование	Математики и компьютерной безопасности	нет	
Криптографический инжиниринг	Математики и компьютерной безопасности	нет	
Программно-аппаратные и технические средства защиты информации	Математики и компьютерной безопасности	нет	
Методы и стандарты оценки защищенности компьютерных систем	Математики и компьютерной безопасности	нет	

Заведующий кафедрой математики и компьютерной безопасности, к.т.н., доцент И. Б. Бураченок