БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Ректор Белорусского
государственного университета
_____ А.Д.Король
10 июня 2024 г.
Регистрационный №УД-13181/уч.

ЗАЩИТА ДАННЫХ И ПРОГРАММ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Учебная программа учреждения 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)

2024 г.

Учебная программа составлена на основе ОСВО 1-98 01 01-2021, учебного плана №Р98-1-206/уч. от 22.03.2022.

СОСТАВИТЕЛЬ:
Зубович К.А., доцент кафедры технологий программирования факультета прикладной математики и информатики Белорусского государственного университета, кандидат физико-математических наук, доцент.

РЕЦЕНЗЕНТ:
Иванченко Ю.И., заведующий научно-исследовательской лабораторией прикладной информатики НИИ ППМИ, кандидат технических наук.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:
Кафедрой технологий программирования БГУ
(протокол № 18 от 16.05.2024)

Научно-методическим советом БГУ
(протокол № 8 от 31.05.2024)

Заведующий кафедрой _____ А.Н. Курбацкий

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи учебной дисциплины

Цель учебной дисциплины - формирование у студентов фундаментальных знаний и приобретение студентами практических навыков в области защиты данных в информационных системах и в области разработки программных продуктов, защищенных от несанкционированного использования.

Задачи учебной дисциплины:

1. Исследование предметной области под названием: «Обеспечение безопасности систем обработки данных»;
2. Изучение методов и средств защиты данных, используемых в настоящее время в информационных системах;
3. Изучение архитектуры компьютера, машинного языка, языков записи алгоритмов, позволяющих строить защиту данных на уровне, наиболее приближенном к аппаратному уровню;
4. Получение знаний, необходимых для успешной работы в качестве специалистов по защите данных и программ в информационных системах.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием.

Учебная дисциплина «Защита данных и программ в информационных системах» относится к дисциплинам специализации компонента учреждения высшего образования.

Связи с другими учебными дисциплинами, включая учебные дисциплины компонента учреждения высшего образования, дисциплины специализации и др.

Содержание учебной программы соответствует уровню подготовки студентов к изучению дисциплины и основывается на следующих учебных дисциплинах: «Основы и методология программирования», «Промышленное программирование» модуля «Программирование» государственного компонента, «Операционные системы» модуля «Информатика и компьютерные системы» государственного компонента, «Теоретические основы информационной безопасности» государственного компонента, «Системное программирование».

Требования к компетенциям

Требования к компетенциям Освоение учебной дисциплины «Защита данных и программ в информационных системах» должно обеспечить формирование следующих компетенций:

Универсальные компетенции:

УК. Владеть основами исследовательской деятельности, осуществлять поиск, анализ и синтез информации;

УК. Решать стандартные задачи профессиональной деятельности на основе применения информационно-коммуникационных технологий;

УК. Работать в команде, толерантно воспринимать социальные, этнические, конфессиональные, культурные и иные различия; УК. Проявлять инициативу и адаптироваться к изменениям в профессиональной деятельности.

Базовые профессиональные компетенции:

БПК. Строить, анализировать и тестировать алгоритмы и программы решения типовых задач обработки информации с использованием структурного, объектно-ориентированного и иных парадигм программирования.

Специализированные компетенции:

СК. Применять навыки проектирования и реализации систем безопасности, осуществлять выбор подходящего криптографического метода защиты типа данных и его реализации

В результате изучения дисциплины студент должен:

знать:

– основные понятия в области защиты информационных систем, правила их построения, основные компоненты подобных систем и принципы их функционирования;

– виды угроз для вычислительных систем, классификацию существующих программных средств, угрожающих целостности, конфиденциальности и доступности защищаемых данных;

– принципы построения и функционирования программного обеспечения, защищенного от несанкционированного использования;

уметь:

– классифицировать угрозы безопасности информационной системы, отличать «вирус» от «троянского коня» и (или) «логической бомбы»;

– разрабатывать простейшие программные продукты, защищенные от несанкционированного использования;

– применять существующие в настоящее время программные средства защиты данных в вычислительных системах (TrueCrypt) и мобильные носители (flash-устройства) с соответствующим программным обеспечением;

иметь навык:

– основными средствами разработки программного обеспечения, ориентированного на защиту данных;

– навыками администрирования операционных систем с элементами обеспечения безопасности информации на примере Windows;

– методами и средствами построения программных средств, защищенных от несанкционированного использования.

Структура учебной дисциплины

Дисциплина изучается в пятом семестре. Всего на изучение учебной дисциплины «Защита данных и программ в информационных системах» отведено:

– для очной формы получения высшего образования – 108 часов, в том числе 68 аудиторных часов, из них: лекции – 34 часа, лабораторные занятия – 30 часов, управляемая самостоятельная работа – 4 часа.

Трудоемкость учебной дисциплины составляет 3 зачетные единицы.

Форма промежуточной аттестации – экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Основные понятия в области защиты данных и программ в информационных системах

Понятие системы, информационной системы. Определение архитектуры системы, основных компонент модельной информационной системы. Понятие и принципы защиты данных. Конфиденциальность, целостность и доступность информации как основные параметры защищенности данных. Постулаты защищенности информационных систем. Необходимые и достаточные условия для построения систем защиты данных и программ.

Тема 2. Классификация угроз, методы и средства защиты данных и программ. Примеры.

Внутренние и внешние угрозы, классификация вредоносного программного обеспечения: вирусы, логические бомбы, «шпионские программы», «трояны» - определение и исследование. Пример разработки «вируса» и соответствующей антивирусной программы.

Тема 3. Архитектура современных компьютерных систем. Низкоуровневое программирование с использованием средств языка ассемблер.

Структура и элементы универсальных вычислительных машин. Центральный процессор. Оперативная память. Основные команды языка ассемблер. Построение программ для 64х-разрядных электронно-вычислительных машин в сравнении с 32х-разрядными. Разработка программ с использованием средств низкоуровневых языков программирования. Примеры программ.

Тема 4. Программные и аппаратные средства защиты данных и программ в информационных системах

Методы и средства защиты данных, основанные на использовании криптографии. Стеганография. Основные стандарты, применяемые в программных средствах шифрования данных (AES, belt, ГОСТ 28147). Применение программного средства TrueCrypt. Аппаратные средства защиты данных на примере использования переносимых устройств хранения данных (flash-накопителей). Программные и аппаратные средства защиты данных от копирования. Примеры.

Тема 5. Построение защищенных вычислительных средств с использованием современных операционных систем, систем управления базами данных и языков программирования

Основные понятия. Администрирование операционных систем в контексте обеспечения безопасности. Фундаментальные концепции безопасности операционных систем: защищенные области, матрицы доступа, механизмы безопасности. Основы безопасности в Microsoft Windows (accounts, group policies, NTFS permission, audit). Примеры администрирования. Различные аспекты безопасности баз данных, их администрирования: permission, roles, views and stored procedures. Разработка программного обеспечения, защищенного от вторжения вредоносных программ и отладчиков.

Тема 6. Обеспечение сетевой безопасности и защита данных с использованием мобильных устройств их хранения

Понятие Firewall и их использование. Фильтрация пакетов. Применение «переносимых устройств» (на примере Flash-устройств Transcend) для защиты от посягательств на доступ к конфиденциальным данным. Возможности «шифрования данных на аппаратном уровне» - мифы и реальности. «Беспроводная и мобильная» безопасность в сетях: GSM-security, Bluetooth-security.

Тема 7. Разработка программного обеспечения систем защиты данных

Определение жизненного цикла программного обеспечения, технологии программирования, ориентированных на создание программ обеспечения защиты данных. Определение требований как основа необходимых и достаточных условий для начала работ по созданию программного обеспечения. Structured Analysis как базис для определения требований. Понятия: принципы хорошего рассказывания, контекст, viewpoint, графическое отображение процессов. Реализация одного из постулатов в области защиты данных: чем на более близком к аппаратному уровню в контексте вычислительной техники осуществлена реализация системы защиты данных, тем она более эффективна – на примере разработки программы, удаляющей саму себя в рамках операционной системы Windows.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Очная (дневная) форма получения высшего образования

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.	Основные понятия в области теории информации и защиты данных в информационных системах	4			4			Письменный опрос в начале каждой лекции, собеседование.
2.	Классификация угроз, методы обнаружения вторжений, методы и средства защиты данных. Примеры	4			4			Собеседование, контрольная работа
3.	Архитектура современных компьютерных систем. Низкоуровневое программирование с использованием средств языка ассемблер.	4			4			Собеседование Отчёт по лабораторной работе
4.	Программные и аппаратные средства защиты данных в информационных системах	6			4		2	Собеседование, проект, контрольная работа
5.	Построение защищенных вычислительных средств с использованием современных операционных							Собеседование, Отчёт по лабораторной работе контрольная работа

	систем, систем управления базами данных и языков программирования	8			4			
6.	Обеспечение сетевой безопасности и защита данных с использованием мобильных устройств их хранения	2			4			Собеседование
7.	Разработка программного обеспечения систем защиты данных	6			6		2	Проект, контрольная работа
	ИТОГО	**34**			**30**		**4**	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Основная литература

1. Таненбаум Э. Архитектура компьютера / Э. Таненбаум, Т. Остин; [пер. с англ. Е. Матвеева].- 6-е изд.- Санкт-Петербург; Москва; Минск : Питер, 2024. - 811 с. - URL: https://ibooks.ru/bookshelf/361850/reading.
2. Организационно-правовое обеспечение информационной безопасности [Электронный ресурс] : электронный учебно-методический комплекс для специальности: 7-06-0421-01 «Юриспруденция» / БГУ, Юридический фак., Каф. Конституционного права, сост. М.С.Абламейко. - Минск: БГУ, 2023. - URL: https://elib.bsu.by/handle/123456789/310228.
3. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие для студ. высших учебных заведений, обуч. по направлению подготовки 10.03.01 "Информационная безопасность (квалификация (степень) "Бакалавр") / Ю. Н. Сычев. - Москва : ИНФРА-М, 2023. - 200 с. - URL: https://znanium.com/catalog/document?id=420080.
4. Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / А. И. Белоус, В. А. Солодуха. - Москва : Техносфера, 2021. - 481 с.
5. Нестеров, С. А. Основы информационной безопасности : учебник / С. А. Нестеров. - Изд. 2-е, стер. - Санкт-Петербург ; Москва ; Краснодар : Лань, 2023. - 320 с. - URL: https://e.lanbook.com/book/370967.

Дополнительная литература

6. Krause M., Tipton H.F. Handbook of information Security Management. – CRC Press LLC. – www.cccure.com
7. David Kim, Michael G. Solomon. Fundamentals of Information Systems Security. - https://books.google.by/books?id=Yb4eDQAAQBAJ&printsec=copyright&redir_esc=y#v=onepage&q&f=false
8. The Red Book: A Roadmap for Systems Security Research. Seventh framework programme.- The SysSec Consortium. – www.syssec-project.eu
9. Intel® 64 and IA-32 Architectures Software Developer’s Manual - Combined Volumes 1-4 - May 2019 (325462-sdm-vol-1-2abcd-3abcd).pdf. https://github.com › master.
10. Бурдаев О.В., М.А. Иванов, И.И. Тетерин. Ассемблер в задачах защиты информации. – М.: Кудиц-Образ, 2004.
11. Куссвюрм Д. Профессиональное программирование на ассемблере x64 с расширениями AVX, AVX2 и AVX-512. – Apress, 2021. – 628 с,

Перечень рекомендуемых средств диагностики и методика формирования итоговой отметки

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

1. Устная форма: собеседование.
2. Письменная форма: контрольная работа.
3. Устно-письменная форма: отчёт по лабораторным работам, проект с устной защитой и оцениванием на основе проектного метода.

Формой промежуточной аттестации по дисциплине учебным планом предусмотрен **экзамен.**

Для формирования итоговой отметки по учебной дисциплине используется модульно-рейтинговая система оценки знаний студента, дающая возможность проследить и оценить динамику процесса достижения целей обучения. Рейтинговая система предусматривает использование весовых коэффициентов для текущей и промежуточной аттестации студентов по учебной дисциплине.

Формирование итоговой отметки в ходе проведения контрольных мероприятий текущей аттестации (примерные весовые коэффициенты, определяющие вклад текущей аттестации в отметку при прохождении промежуточной аттестации):

- отчёт по лабораторной работе – 50%;
- проект – 15 %.
- контрольная работа – 35%

Итоговая отметка по дисциплине рассчитывается на основе отметки текущей аттестации (рейтинговой системы оценки знаний) - 40 %, и экзаменационной отметки – 60 %.

На лекционных занятиях по дисциплине рекомендуется особое внимание обратить на точность формулировок и адекватность перевода англоязычных терминов на русский язык, так как неточные формулировки и перевод зачастую приводит к неверной трактовке тех или иных понятий в сфере безопасности информационных систем. В силу присутствия у студентов старших курсов различных подходов к пониманию материала, в начале семестра следует подробно остановиться на приведении к общему знаменателю их понятийного аппарата.

В силу различного уровня подготовки студентов старших курсов в области вычислительной техники и разработки программного обеспечения систем защиты данных в самом начале курса рекомендуется провести ряд самостоятельных работ и «ролевых игр» для определения этого уровня. И в зависимости от полученного результата варьировать лекционную тематику и степень сложности лабораторных работ. Так, например, в случае высокой квалификации обучаемых в низкоуровневом программировании (отменное знание основ операционных систем и программирования на языке ассемблер) следует больше внимания уделить разработке программного обеспечения систем защиты данных, перенеся данный раздел в начало семестра.

Текущий контроль усвоения знаний в течение семестра по дисциплине «Защита данных и программ в информационных системах» (теоретическая часть курса) рекомендуется осуществлять в виде проведения контрольных. Для закрепления и проверки знаний и умений студентов (практическая часть курса) рекомендуется решение задач по каждому разделу дисциплины в виде выполнения ряда лабораторных работ, постоянного отслеживания процессов выполнения студентами данных им работ непосредственно в компьютерном классе.

Успеваемость студентов в рамках дисциплины «Защита данных и программ в информационных системах» оценивается в конце семестра в форме экзамена в целом по дисциплине.

Примерный перечень заданий для управляемой самостоятельной работы

Тема 4. Программные и аппаратные средства защиты данных в информационных системах (2 ч.).

Классификация вредоносных программ.

Средства защиты от вредоносных программ.

Разработать простейшую антивирусную программу.

(Форма контроля – проект по разработке программного обеспечения, обеспечивающее защиту от вируса DHog68).

Тема 7. Разработка программного обеспечения систем защиты данных (2 ч.).

Зашита программных средств и данных от несанкционированного копирования и использования.

Структура исполнимых модулей.

Разработать программу, защищенную от исследования под отладчиком.

(Форма контроля – проект по созданию программного средства защиты от несанкционированного копирования, средства, которое невозможно использовать на «чужом» компьютере, в другой папке, под другим именем).

Описание инновационных подходов и методов к преподаванию учебной дисциплины

При организации образовательного процесса большинства занятий используется **практико-ориентированный подход**, который предполагает освоение содержания образования через решение практических задач; приобретение навыков эффективного выполнения разных видов профессиональной деятельности.

При организации образовательного процесса используется **метод группового обучения**, который представляет собой форму организации учебно-познавательной деятельности обучающихся, предполагающую функционирование разных типов малых групп, работающих как над общими, так и специфическими учебными заданиями.

При проведении занятий в компьютерном классе основной формой работы является работа студентов над заданиями под руководством и контролем преподавателя. В основном, предполагается, что вариант задания является индивидуальным, т. е., рассчитанным на выполнение одним студентом, в некоторых случаях, например, проектных работах, задание может выполняться небольшой группой студентов (2-3 студента). Преподаватель должен оперативно консультировать выполнение заданий и принимать выполненное задание (оценивать результаты его выполнения) посредством визуальной проверки полученных результатов и собеседованием со студентом (группой студентов).

В силу различного уровня готовности студентов к восприятию новых понятий, на занятиях по дисциплине рекомендуется при необходимости проводить дополнительные консультации в малых группах студентов для объяснения и закрепления сложного материала

Методические рекомендации по организации самостоятельной работы

Условия для самостоятельной работы студентов, в частности, для развития навыков самоконтроля, способствующих интенсификации учебного процесса, обеспечиваются наличием и полной доступностью электронных (и бумажных) документов с указанием ссылок на первоисточники в рамках сети Интернет.

Использование при выполнении самостоятельной работы в процессе обучения принципа «трех компасов», когда для получения адекватного результата требуется изучение трех источников:

1. Средства массовой информации (книги, Интернет, лекции преподавателя, знания других студентов, знакомых, родственников и т.д. и т.п.)
2. «Здравый смысл» - собственные познания.
3. Результаты взаимодействия по решаемой проблеме с вычислительной техникой (результаты выполнения программ или результаты использования существующих программных средств).

Применение в процессе обучения подхода, основанного на том, что для организации самостоятельной работы и определения «уровня компетенции студентов» в процессе чтения лекций и при выполнении студентами лабораторных занятий, преподавателем выдвигаются «неверные» в контексте «трех компасов» утверждения (заведомо ложные»), которые должны быть опровергнуты обучаемыми.

Примерный перечень вопросов к экзамену

1. Понятие информационной системы. Основные толкования. Постулаты безопасности информационных систем.
2. Программа «клавиатурный шпион». Обработка клавиатуры.

3. Понятие и принципы защиты данных. Конфиденциальность, целостность и доступность информации как основные параметры защищенности данных.

4. Программа, уничтожающая сама себя.

5. Угрозы безопасности систем защиты данных. Классификация угроз по различным признакам. Преднамеренные и непреднамеренные угрозы.

6. Программа, изменяющая сама себя.

7. Понятие «атаки». Каналы несанкционированного доступа к данным.

8. Программа вывода на экран изображений «управляющих символов» и их шестнадцатеричных кодов.

9. «Внутренние и внешние угрозы, классификация вредоносного программного обеспечения: вирусы, логические бомбы, «шпионские программы», «трояны» - определение и исследование.

10. Самоизменяющаяся программа, возводящая значение цифры в куб, хотя изначально была составлена для получения квадрата.

11. «Резидентные программы, средства их обнаружения и локализации, описание основных антивирусных программных средств на примере антивирусного программного средства. Пример разработки «вируса».

12. Программа, осуществляющая ввод с клавиатуры символа и вывод на экран кода этого символа в шестнадцатеричном представлении. Размер программы не должен превышать 24 байта.

13. Классификация вирусов. Подходы и различия. Классы вирусов. Пример разработки «вируса».

14. Программа, осуществляющая ввод с клавиатуры однозначного числа и вывода на экран остатка от деления его на число 10. Размер программы не должен превышать 24 байта.

15. Средства борьбы с угрозами. Управление доступом.

16. Программа вывода на экран своего сокращенного имени.

17. Программа вывода на экран своего полного имени.

18. Средства борьбы с угрозами. Защита данных в «операционных оболочках» на примере Windows.

19. Программа вывода на экран дескриптора файла выполняемой программы.

20. Средства борьбы с угрозами. Защита данных в программных средствах Microsoft Word и Microsoft Excel.

21. Программа вывода на экран значения атрибута файла выполняемой программы.

22. Средства борьбы с угрозами. Защита данных в системах управления базами данных на примере Microsoft Access.

23. Программа, удаляющая сама себя.

24. Средства борьбы с угрозами. Защита данных от несанкционированного воздействия с применением программно-технических средств защиты.

25. Программа, которая изменяет заданный выполнимый модуль, хранящийся на внешнем запоминающем устройстве.

26. Средства борьбы с угрозами. Защита данных от несанкционированного воздействия с применением программно-технических средств защиты.

27. Программа, которая позволяет ввести пароль и сравнить его с паролем, заданным в самой программе.

28. Средства борьбы с угрозами. Защита данных от несанкционированного воздействия с применением аппаратно-программных средств переносимых flash-устройств.

29. Программа, которая позволяет удалить файл, имя которого вводится с клавиатуры.

30. Средства борьбы с угрозами. Защита данных от несанкционированного воздействия с применением аппаратно-программных средств ЭВМ.

31. Программа, которая позволяет изменить саму себя в процессе своего исполнения.

32. Структура исполнимых модулей типа Com и Exe. Понятие PSP. Структура PSP. Доступ к данным о системном окружении выполняемой программы.

33. Программа, которая позволяет вывести на экран ИЗОБРАЖЕНИЯ ВСЕХ символов кодировочной ASCII – таблицы, используемой в данный момент на ЭВМ.

34. Средства борьбы с угрозами. Защита данных от несанкционированного воздействия с применением программно-технических изделий. Краткая их характеристика.

35. Программа, которая позволяет выводить на экран скэн-коды нажатых на клавиатуре клавиш. Понятие резидентной программы.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УО

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)
Введение в информационную безопасность	Кафедра технологий программирования	Изменений не требуется	Протокол №18 от 16.05.2024

Заведующий кафедрой
Доктор технических наук
Профессор А.Н. Курбацкий

16 мая 2024 г.

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ

на _____/_____ учебный год

№№ Пп	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры

_____(протокол № ____ от _____ 202_ г.)

(название кафедры)

Заведующий кафедрой

_____ _____

(ученая степень, ученое звание) (И.О.Фамилия)

УТВЕРЖДАЮ

Декан факультета

_____ _____

(ученая степень, ученое звание) (И.О.Фамилия)