Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Тверской государственный университет»

Утверждаю:
Руководитель ООП
Н.А. Семыкина
«4» 09 2023 г.

Рабочая программа дисциплины (с аннотацией)

Программно-аппаратные средства защиты информации от несанкционированного доступа

Специальность

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»

Для студентов очной формы обучения

СПЕЦИАЛИТЕТ

Для студентов 4 курса ОФО

Составитель:
Семыкина Н. А.

Тверь 2023

I. Аннотация

1. Цель и задачи дисциплины

Целью изучения дисциплины является теоретическая и практическая подготовка специалистов к деятельности, связанной с построением современных систем защиты информации в операционных системах и вычислительных сетях.

Задачами освоения дисциплины являются:

1) изучение принципов построения подсистем защиты в сетях различной архитектуры;

2) изучение средств, методов, алгоритмов, программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;

3) изучение принципов функционирования современных систем идентификации и аутентификации;

4) изучение программных продуктов от несанкционированного доступа, модификации и изучения в автоматизированных системах.

2. Место дисциплины в структуре ООП

Данная дисциплина входит в вариативную часть учебного плана и является дисциплиной по выбору, связана с другими дисциплинами образовательной программы: «Основы информационной безопасности», «Аппаратные средства вычислительной техники», «Операционные системы».

Дисциплины, для которых освоение данной дисциплины необходимо как предшествующее: «Сети и системы передачи информации», «Организационное и правовое обеспечение информационной безопасности», «Основы построения защищенных компьютерных сетей», «Научно-исследовательская работа», «Проектно-технологическая практика», «Преддипломная практика».

3. Объем дисциплины: 5 зачетные единицы, 180 академических часов, в том числе:

контактная аудиторная работа: лекции – 34 часов, в т.ч. практическая подготовка – 0 часов;

практические занятия – 34 часов, в т.ч. практическая подготовка – 0 часов;

лабораторные занятия – 17 часов, в т.ч. практическая подготовка – 4 часа;

самостоятельная работа: 95 часов, в том числе контроль 27 часов.

4. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	Планируемые результаты обучения по дисциплине
ПК-3 Способен применять методы и методики оценивания безопасности компьютерных систем при проведении контрольного анализа системы защиты	**ПК-3.1** Проводит анализ угроз информационной безопасности в сетях электросвязи
	ПК-3.2 Проверяет работоспособность и эффективность применяемых программно-аппаратных средств защиты информации

	ПК-3.3 Проводит анализ безопасности компьютерных систем
ПК-5 Способен производить установку, наладку, тестирование и обслуживание программно-аппаратных средств обеспечения информационной безопасности компьютерных систем	**ПК-5.1** Производит эксплуатацию информационно-аналитических систем в защищенном исполнении
	ПК-5.2 Тестирует системы защиты информации автоматизированных систем
	ПК-5.3 Разрабатывает эксплуатационную документацию на системы защиты информации автоматизированных систем

5. Форма промежуточной аттестации и семестр прохождения – экзамен в 7 семестре.

6. Язык преподавания русский**.**

II. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

Очная форма обучения

Учебная программа – наименование разделов и тем	Всего (час.)	Контактная работа (час.)			Самостоятельная работа, в том числе Контроль (час.)
		Лекции	Практические занятия		
			всего	в т.ч. практическая подготовка	
Раздел 1. Нормативно-правовые и технические требования к программно-аппаратным средствам защиты информации	28	4	4	0	20
Раздел 2. Программно-аппаратные средства защиты информации от несанкционированного доступа	51	10	14	2	25

Раздел 3. Программные средства защиты информации в операционных системах и базах данных.	51	10	14	2	25
Раздел 4. Аппаратные средства защиты информации, средства криптографической защиты, биометрические средства идентификации	50	10	15	0	25
ИТОГО	180	34	47	4	95

III. Образовательные технологии

Учебная программа – наименование разделов и тем	Вид занятия	Образовательные технологии
Раздел 1. Нормативно-правовые и технические требования к программно-аппаратным средствам защиты информации	лекция практическое	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция, кейс-технология, технология развития креативного мышления.
Раздел 2. Программно-аппаратные средства защиты информации от несанкционированного доступа	лекция практическое	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция, кейс-технология, технология развития креативного мышления.
Раздел 3. Программные средства защиты информации в операционных системах и базах данных.	лекция практическое	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция, кейс-технология, технология развития креативного мышления.

Раздел 4. Аппаратные средства защиты информации, средства криптографической защиты, биометрические средства идентификации	лекция практическое	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция, кейс-технология, методы группового решения творческих задач.

IV. Оценочные материалы для проведения текущей и промежуточной аттестации

Оценочные материалы для проведения <u>текущей аттестации</u>

<u>Задания для практических (семинарских) занятий</u>

Раздел I.

Задание 1 (ПК-3.1; ПК-3.2; ПК-3.3): Перечислить традиционные методы, технологии и средства защиты информации в ПЭВМ. Определите недостатки традиционных методов и средств защиты информации в ПЭВМ.

Задание 2 (ПК-3.1; ПК-3.2; ПК-3.3): Определить нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.

Раздел II.

Задание 1 (ПК-3.1; ПК-3.2; ПК-3.3): Поясните модель канала утечки информации.

Задание 2 (ПК-3.1; ПК-3.2; ПК-3.3): В качестве примеров отдельных программ, повышающих защищенность от НСД, можно привести утилиты из пакета Norton Utilities, такие как программа шифрования информации при записи на диск Diskreet или Secret disk, программа стирания информации с диска WipeInfo, программа контроля обращения к дискам DiskMonitor и др. Опишите одно из программных средств, повышающих защищенность от НСД.

Раздел III.

Задание 1 (ПК-5.1; ПК-5.2; ПК-5.3): Проведите исследование реестра Windows для нахождения следов активности вредоносного ПО.

Задание 2 (): Угроза несанкционированного копирования информации блокируется методами, которые могут быть распределены по двум группам: ï методы, затрудняющие считывание скопированной информации; ï методы, препятствующие использованию информации. Приведите примеры методов каждой группы. Сделайте сравнительный анализ основных методов защиты от копирования.

Задание 3 (ПК-5.1; ПК-5.2; ПК-5.3): Защитите созданную базу данных с помощью Мастера. MS Access предоставляет средства распределенного доступа к базе данных. С одним файлом могут одновременно работать большое количество пользователей, обладающих разными правами: одни могут только просматривать таблицы, другие – только вносить новые данные, и лишь администраторы базы обладают полным доступом. Разделите доступ для двух пользователей – один сможет только просматривать данные (читать), другой будет обладать полным доступом. Опишите этапы защиты базы данных с помощью Мастера.

Раздел VI.

Задание 1 (ПК-5.1; ПК-5.2; ПК-5.3): *Установка аппаратной части комплекса «Соболь»*

Вскройте корпус системного блока и выберите свободный слот системной шины PCI/PCI-Express/ Mini PCI-Express.

Переключите плату комплекса «Соболь» в режим инициализации. Для этого снимите перемычку, установленную на разъеме платы **J0**, / установите переключатель платы SW в положение OFF.

Установите в свободный слот системной шины Mini PCI-E плату комплекса "Соболь" (см. Рисунок):

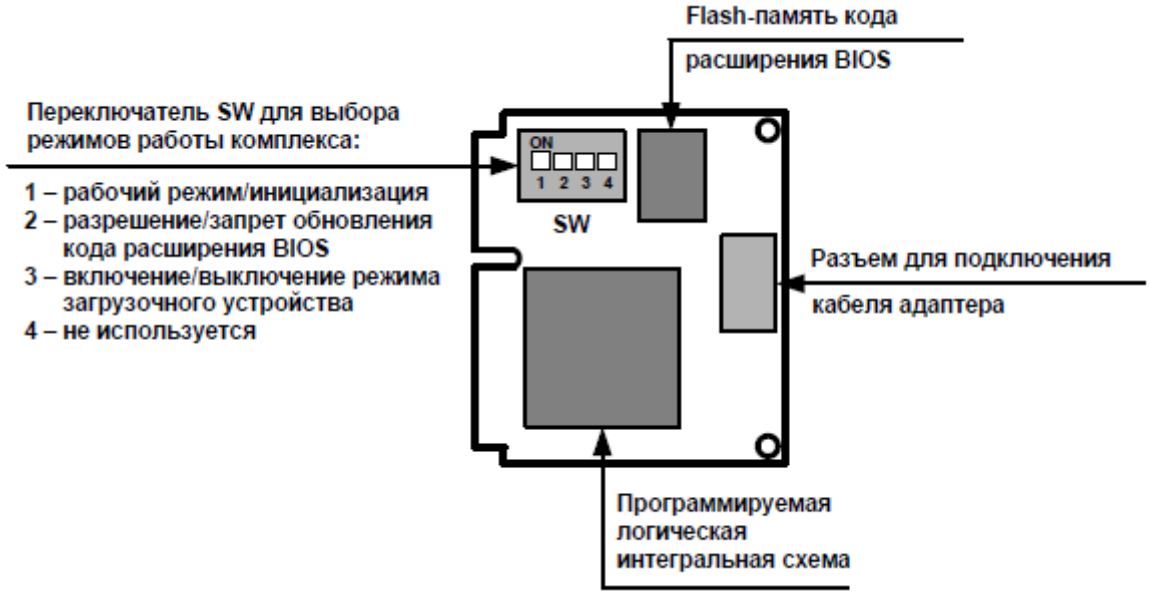

Рисунок.

Подключите первый штекер кабеля механизма сторожевого таймера, входящего в комплект поставки, к разъему платы WD. Затем подключите второй

штекер этого кабеля к разъему Reset, расположенному на материнской плате. Аккуратно вставьте в разъем плату комплекса «Соболь».

Задание 2 (ПК-5.1; ПК-5.2; ПК-5.3): *Настройка аппаратной идентификации*
После установки соответствующего драйвера электронного идентификатора Рутокен следует настроить аппаратную идентификацию и назначить аппаратный идентификатор пользователю.

Оценочные материалы для проведения промежуточной аттестации

Проверяемые индикаторы достижения компетенций: ПК-3.1; ПК-3.2; ПК-3.3; ПК-5.1; ПК-5.2; ПК-5.3.

Каждый студент отвечает на вопросы теста и дает развернутый ответ на теоретический вопрос.

Примерные вопросы к экзамену

1.. Нормативно-правовые и технические требования к программно-аппаратным средствам защиты информации.
2.. Понятие несанкционированного доступа (НСД) к информации
3.. Концепция защиты от НСД к информации
4.. Основные каналы утечки информации в локальной ПЭВМ
5.. Модель нарушителя при локальном НСД
6.. Основные каналы утечки информации в рабочей станции
7.. Показатели защищенности средств вычислительной техники от несанкционированного доступа. 8. Модель нарушителя при удаленном НСД
8.. Методы и средства защиты информации от НСД в локальных ПЭВМ
9.. Методы и средства защиты информации от НСД на рабочих станциях в сети
10. Перечислить традиционные методы, технологии и средства защиты информации в ПЭВМ
11. Недостатки традиционных методов и средств защиты информации в ПЭВМ
12. Стандарты безопасности и их влияние на проектирование и разработку программно-аппаратных средств защиты информации.
13. Принципы сертификации средств защиты информации
14. Основы разработки и проектирования программно-аппаратных комплексов обеспечения информационной безопасности.
15. Способы НСД к информации и защиты от него в компьютерных системах.
16. Средства и методы ограничения доступа к файлам.
17. Классификация средств хранения ключей и идентифицирующей информации.
18. Методы противодействия динамическим способам снятия защиты программ от копирования.
19. Методы защиты программ от исследования.
20. Подходы к задаче защиты от копирования программ.
21. Общая характеристика и классификация компьютерных вирусов.
22. Общая характеристика средств нейтрализации компьютерных вирусов.
23. Защита на уровне загрузчиков операционной среды.
24. Архитектура подсистемы безопасности ОС Windows.
25. Разграничение прав пользователей в ОС Windows.
26. Аудит событий безопасности в ОС Windows.

27. Домены безопасности.
28. Микроядерная архитектура с точки зрения создания защищенных операционных систем.
29. Аутентификация пользователей при локальном и удаленном доступе к КС.
30. Средства обеспечения целостности и конфиденциальности при передаче информации по каналам связи.
31. Технология и классификация VPN.
32. Требования к межсетевым экранам. 19. Методы поиска уязвимостей.
33. Симметричные и асимметричные алгоритмы шифрования информации.
34. Функции удостоверяющего центра.
35. Структура удостоверяющего центра.
36. Концепция иерархии ключей.
37. Генерация и хранение ключей.
38. Распределение ключей
39. Использование программно-аппаратных средств для защиты информации.
40. Дискретное, мандатное и ролевое разграничение доступа к объектам КС.
41. Способы идентификации и аутентификации субъектов КС.
42.. Способы фиксации фактов доступа к файлам. Журналы доступа.
43. Способы защиты информации на съемных дисках.
44. Основные схемы резервного копирования.
45. Программные закладки и их воздействие на компьютеры.
46. Защита данных от разрушающих программных воздействий.
47. Формирование и поддержка замкнутой программной среды.
48. Классификация средств исследования программ.
49. Методы и средства защиты от несанкционированного копирования.
50. Юридические аспекты несанкционированного копирования программ.
51. Защита массивов информации от изменения.
52. Формирование хеш-функций, требования к построению и способы реализации.
53. Формальные модели безопасности ОС.
54. Реализация механизмов безопасности на аппаратном уровне.
55. Архитектура подсистемы безопасности ОС Windows.
56. Создание защищенной операционной системы
57. Принцип работы систем обнаружения вторжений.
58. Анализ защищенности системы при помощи сканера безопасности.
59. Взаимная проверка подлинности пользователей.
60. Программно-аппаратные средства криптографической защиты информации.
61. Требования, предъявляемые к удостоверяющему центру.
62. Протокол аутентификации и распределения ключей для симметричных криптосистем.
63.. Протокол для асимметричных криптосистем с использованием сертификатов открытых ключей.
64. Атаки и методы защиты на уровне СУБД.
65. Модели безопасности, применяемые при построении защиты в СУБД.
66. Транзакция и восстановление.
67. Технологии тиражирования и синхронизации данных

68. Кластерная организация серверов баз данных.
69. Стандарты безопасности и их роль.
70. Порядок сертификации средств защиты информации.
71. Основы разработки и проектирования программно-аппаратных комплексов обеспечения информационной безопасности.

Вид и способ проведения промежуточной аттестации: индивидуальный устный опрос сочетается с самостоятельной практической работой студента.

Критерии оценивания и шкала оценивания:

Максимально возможное количество баллов – **3** балла. Для получения зачета необходимо ответить на вопросы теста и дать ответ на теоретический вопрос с суммарной оценкой не менее 2-х балов.

3 балла:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Факты и примеры в полном объеме обосновывают выводы. Имеется решение теста верное от 85 – 100% всех заданий.

2 балла:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Ответ не содержит фактических ошибок. Верно даны ответы на 70-84% тестовых заданий.

1 балл:

Ответ демонстрирует знание и корректное использование терминологии. Правильные решения тестовых заданий составляют от 41-69%.

0 баллов:

В ответе преобладают рассуждения общего характера И/ИЛИ содержит существенные фактические ошибки, искажающие смысл. Правильные тестовые ответы составляют менее 40%.

V. Учебно-методическое и информационное обеспечение дисциплины

1) Рекомендуемая литература

а) Основная литература

Бутин А. А. Программно-аппаратные средства защиты информации [Электронный ресурс] : учебное пособие / А. А. Бутин, Н. И. Глухов, С. И. Носков. - 2-е изд., перераб. и доп. - Иркутск : ИрГУПС, 2022. - 92 с. Р: https://e.lanbook.com/book/342113

Жмуров Д. Б. Программно-аппаратные средства защиты информации [Электронный ресурс] : учебное пособие / Д. Б. Жмуров, С. В. Жуков. - Самара : Самарский университет, 2022. - 80 с. – Режим доступа: https://e.lanbook.com/book/336515

Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — URL: https://urait.ru/bcode/471159

б) Дополнительная литература:

Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс]: научно-техническое издание / А.И. Астайкин [и др.]. — Электрон. текстовые данные. — Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015. — 224 c. — 978-5-9515-0305-3. — Режим доступа: http://www.iprbookshop.ru/60959.html

Фефилов А. Д. Методы и средства защиты информации в сетях : практическое пособие / А. Д. Фефилов. - Москва : Лаборатория книги, 2011. - 105 с. : ил., табл. - Режим доступа: : https://biblioclub.ru/index.php?page=book&id=140796

Разрушающие программные воздействия: учебно-методическое пособие для вузов. [Электронный ресурс] : учеб.-метод. пособие / А.Б. Вавренюк [и др.]. — Электрон. дан. — М. : НИЯУ МИФИ, 2011. — 328 с. — Режим доступа: http://e.lanbook.com/book/75792

2) Программное обеспечение

Google Chrome	бесплатно
Kaspersky Endpoint Security 10 для Windows	Акт на передачу прав ПК545 от 16.12.2022
Lazarus	бесплатно
OpenOffice	бесплатно
Многофункциональный редактор ONLYOFFICE бесплатное ПО	бесплатно
ОС Linux Ubuntu бесплатное ПО	бесплатно

3) Современные профессиональные базы данных и информационные справочные системы

1. ЭБС Лань https://e.lanbook.com/ Договор № 4-е/23 от 02.08.2023 г.
2. ЭБС Znanium.com https://znanium.com/ Договор № 1106 эбс от 02.08.2023 г.
3. ЭБС Университетская библиотека online https://biblioclub.ru Договор № 02-06/2023 от 02.08.2023 г.
4. ЭБС ЮРАЙТ https://urait.ru/ Договор № 5-е/23 от 02.08.2023 г.
5. ЭБС IPR SMART https://www.iprbookshop.ru/ Договор № 3-е/23К от 02.08.2023 г.

4) Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины:

https://cyberleninka.ru/ научная электронная библиотека «Киберленинка».

www.fstec.ru Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

http://www.intuit.ru/ Национальный Открытый Университете «ИНТУИТ»

http://www.cisco.com/c/ru_ru/index.html Сетевой Академии Cisco

VI. Методические материалы для обучающихся по освоению дисциплины

Методические рекомендации по организации самостоятельной работы студентов

На лекциях будет представлен необходимый теоретически материал по темам и представлены практические задания для решения на занятиях в аудитории под руководством преподавателя и самостоятельно. Многие задачи являются стандартными и имеют уже готовые шаблоны (алгоритмы) решения, тем не менее, для получения большего познавательного и учебного эффекта, рекомендуется написание собственного оригинального кода.

Самостоятельная работа студентов в рамках данной дисциплины в основном состоит в подготовке к практическим занятиям и работе с разными источниками. Освоению учебного материала большую помощь окажет личный творческий подход, связанный с дополнительным просмотром материала по отдельным темам.

Самостоятельная работа является необходимой на всей стадиях и при всех формах изучения предмета. Важно помнить, что часы для самостоятельной работы, из всего объема времени затраченного на дисциплину, будут превосходить иные виды работ. Важно продумать стиль фиксации нового и важного материала.

Рекомендуется немедленно обсуждать любые возникшие в процессе обучения вопросы, проблемы и неясности с преподавателем, не откладывая это обсуждение до контрольной точки. Проконсультироваться с преподавателем можно во время и после практических занятий, во время консультаций, а также по электронной почте и в личном кабинете электронной образовательной среды (LMS).

Требования к рейтинг-контролю для студентов очной формы обучения.

Текущая работа студентов очной формы обучения оценивается в 60 баллов, которые распределяются между двумя модулями (периодами обучения) следующим образом:

Модуль (период обучения)	Максимальная сумма баллов в модуле	Максимальная сумма баллов за работу на практических занятиях	Реферирование, представление научной статьи, создание и отладка кода	Максимальный балл за рейтинговую контрольную работу
1	30	10	5	15
2	30	10	5	15

Правила формирования рейтинговой оценки и шкалу пересчета рейтинговых баллов в оценку на экзамене см. в «Положении о рейтинговой системе обучения в ТвГУ»:
https://tversu.ru/sveden/files/204-R_Pologhenie_o_reytingovoy_sisteme_obucheniya_v_TvGU.pdf

VII. Материально-техническое обеспечение

Учебный процесс по данной дисциплине проводится в аудиториях, оснащенных мультимедийными средствами обучения. Для организации самостоятельной работы студентов необходимо наличие персональных компьютеров с доступом в Интернет.

Наименование специальных* помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**	**Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа**
Помещение для самостоятельной работы, учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, практики Компьютерный класс 203а 170002, г.Тверь, Садовый пер-к, д. 35.	Столы, стулья, переносной ноутбук, компьютеры	Google Chrome-бесплатно; Kaspersky Endpoint Security 10 для Windows-Акт на передачу прав ПК545 от 16.12.2022; Lazarus –бесплатно; OpenOffice – бесплатно; Многофункциональный редактор ONLYOFFICE бесплатное ПО- бесплатно; ОС Linux Ubuntu бесплатное ПО- бесплатно
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, у*чебная аудитория* 203, 224, 170002, г.Тверь, Садовый пер-к, д. 35	Столы, стулья, переносной ноутбук, проектор	Google Chrome-бесплатно; Kaspersky Endpoint Security 10 для Windows-Акт на передачу прав ПК545 от 16.12.2022; Lazarus –бесплатно; OpenOffice – бесплатно; Многофункциональный редактор ONLYOFFICE бесплатное ПО- бесплатно; ОС Linux Ubuntu бесплатное ПО- бесплатно

Наличие учебно-наглядных пособий, презентаций для проведения занятий лекционного и семинарского типа, обеспечивающих тематические иллюстрации.

VIII. Сведения об обновлении рабочей программы дисциплины

№п.п.	**Обновленный раздел рабочей программы дисциплины (или модуля)**	**Описание внесенных изменений**	**Дата и протокол заседания кафедры, утвердившего изменения**

1.	I - VIII	Создание РПД в соответствии с новым стандартом	Протокол № 10 от 29.06.2021
2.	V. Учебно-методическое и информационное обеспечение дисциплины	Обновление списков ПО. Обновление ссылок из ЭБС.	Протокол № 1 от 1.09.2023