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)

Модели безопасности компьютерных систем

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 освоения дисциплины - раскрытие содержания основных понятий и формальных моделей обеспечения безопасности компьютерных систем, а также сформирование теоретико-методологических основ профессиональной деятельности в сфере компьютерной безопасности в контексте всех трех ее составляющих видов — производственно-технологической, организационно-управленческой и экспериментально-исследовательской.

Задачами освоения дисциплины являются:

1) получение базовых знаний и умений, связанных с основными понятиями в сфере компьютерной безопасности;

2) изучение общих принципов анализа и обоснования моделей, методов и механизмов обеспечения компьютерной безопасности;

3) освоение методологии анализа архитектурных (схемно-технических) и программно-алгоритмических решений, применяемых в системах защиты информации современных компьютерных систем.

2. Место дисциплины в структуре ООП

Данная дисциплина входит в обязательную часть учебного плана, связана с другими дисциплинами образовательной программы: «Основы информационной безопасности», «Компьютерные сети»», «Операционные системы».

Дисциплины, для которых освоение данной дисциплины необходимо как предшествующее: «Защита в операционных системах», «Научно-исследовательская работа», «Проектно-технологическая практика», «Преддипломная практика».

3. Объем дисциплины: 4 зачетные единицы, 144 академических часов, в том числе:

контактная аудиторная работа: лекции – 30 часов, в т.ч. практическая подготовка – 0 часов;

лабораторные занятия – 30 часов, в т.ч. практическая подготовка – 4 часа;

самостоятельная работа: 57 часа, 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
ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	**ОПК-8.2** Осуществляет моделирование безопасности компьютерных систем, в том числе моделирование управления доступом и информационными потоками в компьютерных системах
ОПК-11. Способен разрабатывать политики безопасности, политики	**ОПК-11.1.** Использует основные формальные модели дискреционного, мандатного, ролевого управления

управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	доступом, модели изолированной программной среды и безопасности информационных потоков
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	**ОПК-6.1.** Разрабатывает модели угроз и модели нарушителя компьютерных систем
	ОПК-6.2. Разрабатывает проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации
	ОПК-6.3. Определяет политику контроля доступа работников к информации ограниченного доступа
	ОПК-6.4. Применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы
ОПК-16. Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях	**ОПК-16.1.** Применяет защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях
	ОПК-16.2. Осуществляет меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты

5. Форма промежуточной аттестации и семестр прохождения – экзамен в 8 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. Исходные положения теории компьютерной безопасности	19	2	2	0	15
Раздел 2. Классические модели безопасности компьютерных систем. Математические основы моделей безопасности	57	16	14	2	25
Раздел 3. Модели компьютерных систем с ролевым управлением. Модели изолированной программной среды	45	10	8	2	25
Раздел 4. Стандарты в информационной безопасности	23	2	2	0	19
ИТОГО	144	30	26	4	84

III. Образовательные технологии

Учебная программа – наименование разделов и тем	Вид занятия	Образовательные технологии
Раздел 1. Исходные положения теории компьютерной безопасности	лекция практическое	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция.
Раздел 2. Классические модели безопасности компьютерных систем. Математические основы моделей безопасности	лекция практическое	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция, кейс-технология, технология развития креативного мышления

Раздел 3. Модели компьютерных систем с ролевым управлением. Модели изолированной программной среды	лекция практическое	Дискуссионные технологии, кейс-технология, методы группового решения творческих задач.
Раздел 4. Стандарты в информационной безопасности	лекция практическое	Дискуссионные технологии, кейс-технология, методы группового решения творческих задач

IV. Оценочные материалы для проведения текущей и промежуточной аттестации

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

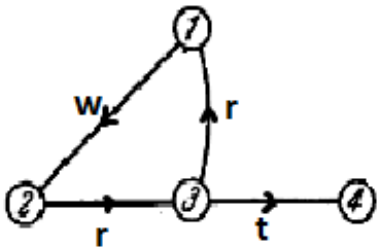
<u>Задания для практических (семинарских) занятий</u>

Раздел I.

Задание 1 (ОПК-6.3; ОПК-6.4): Сформулируйте основную аксиому теории компьютерной безопасности.

Раздел II.

Задание 1 (ОПК-6.1; ОПК-8.2; ОПК-11.1): Построить де-юре-замыкание графа доступов



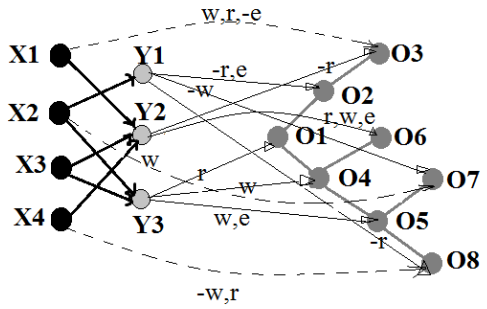
Задание 2 (ОПК-6.1; ОПК-8.2; ОПК-11.1): Пусть имеется мандатная система доступа, в которой решетка уровней безопасности Λ_L является линейной и имеет три уровня – $l1$, $l2$, $l3$; $l1>l2>l3$.

На предприятии есть следующие должности: директор, заместитель директора, ведущий инженер и главный конструктор, в подчинении у них инженеры и специалисты. Имеется следующая система объектов доступа: документ «Новые разработки конструкторского бюро предприятия»; Ведомость покупных изделий, Ведомость технического проекта, Эксплуатационные документы, Чертежи деталей, Инструкция.

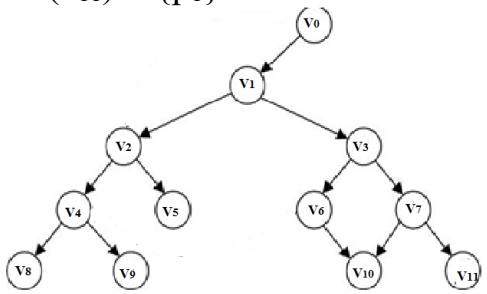
Обосновать и составить систему уровней допусков пользователей, грифов секретности объектов доступа и матрицу доступа $\boldsymbol{A}[\boldsymbol{u},\boldsymbol{o}]$..

Раздел III.

Задание 1 (ОПК-6.1; ОПК-8.2; ОПК-11.1): Пусть имеется иерархически организованная система объектов доступа О и система субъектов Х, объединенных в рабочие группы. Вхождение пользователей в рабочие группы показаны на рисунке. Определите общий коэффициент дублирования прав доступа в системе по записи и коэффициент дублирования прав доступа по записи для пользователя x_4 .



Задание 2 (ОПК-6.1; ОПК-8.2; ОПК-11.1): Пусть имеется система иерархически организованных ролей ***V***. Ролям назначены полномочия из конечного множества. Определить полномочия роли $\mathbf{v_1}$ и роли $\mathbf{v_3}$. $P(v_0) = \{p_7\}$, $P(v_1) = \{p_3\}$, $P(v_2) = \{p_2, p_4\}$, $P(v_3) = \{p_5\}$, $P(v_4) = \{p_8\}$, $P(v_5) = \{p_6, p_8\}$, $P(v_6) = \{p_8\}$, $P(v_7) = \{p_1\}$, $P(v_8) = \{p_2\}$, $P(v_9) = \{p_6\}$, $P(v_{10}) = P(v_{11}) = \{p_1\}$.



Раздел IV.

Задание 1 (ОПК-6.2; ОПК-6.3; ОПК-6.4): Приведите список мероприятий по обеспечению защиты информации в ГИС.

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

Проверяемые индикаторы достижения компетенций: ОПК-6.1; ОПК-6.2; ОПК-6.3; ОПК-6.4; ОПК-8.2; ОПК-11.1; ОПК-16.1; ОПК-16.2.

Каждый студент решает индивидуальное задание и отвечает на теоретический вопрос.

Примерные вопросы к экзамену

1. Безопасность информации. Безопасности функций КС.
2. Угрозы безопасности в компьютерных системах. Классификация методов защиты информации в компьютерных системах. Основные критерии оценки надежности.
3. Принципы политики безопасности. Виды политики безопасности.
4. Модель матрицы доступов HRU. Элементарные операторы. Безопасность системы HRU.
5. Модель распространения прав доступа TAKE – GRANT. Команды модели TAKE – GRANT. Санкционированное получение прав доступа.
6. Похищение прав доступа в модели TAKE – GRANT.
7. Расширенная модель TAKE-GRANT. Де-факто правила расширения модели Take-Grant.
8. Построение замыкания графа доступов и информационных потоков.
9. Алгоритм построения tg-замыкания.

10. Алгоритм построения де-юре-замыкания.
11. Алгоритм построения де-факто-замыкания. Определение стоимости путей
12. Модель Белла – ЛаПадулы. Основные правила, гарантирующих безопасность. Основная теорема безопасности.
13. Модель Кена Биба. Основные правила, гарантирующих безопасность.
14. Модель систем военных сообщений. Постулаты безопасности модели MMS. Неформальные свойства модели MMS.
15. Базовая модель Ролевого Разграничения Доступа (РРД).
16. Модель администрирования РРД. Администрирование множеств авторизованных ролей пользователей. Администрирование множеств прав доступа, которыми обладают роли. Администрирование иерархии ролей.
17. Модели безопасности на основе тематической политики. Основные способы тематической классификации. Тематические решетки: при дескрипторной тематической классификации и при иерархической тематической классификации.
18. Модель тематико-иерархического разграничения доступа. Критерий безопасности.
19. Правила санкционированных переходов системы с помощью монитора безопасности объектов (МБО).
20. Субъектно – ориентированная модель изолированной программной среды.
21. Стандарты в 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 – **5** баллов. Для получения положительной оценки на экзамене необходимо выполнить задачу и ответить на теоретический вопрос с суммарной оценкой не менее 3-х балов.

5 баллов:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Факты и примеры в полном объеме обосновывают выводы. Имеется полное верное решение задачи, включающее правильный ответ.

4 балла:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Ответ не содержит фактических ошибок. Дано верное решение задачи, но в решении имеются неверные записи И/ИЛИ арифметические ошибки.

3 балла:

Ответ демонстрирует знание и корректное использование терминологии. Решение содержит фактические ошибки, не искажающие общего смысла.

0-2 баллов:

В ответе преобладают рассуждения общего характера И/ИЛИ содержит существенные фактические ошибки, искажающие смысл. Решение не дано ИЛИ дано неверное решение.

V. Учебно-методическое и информационное обеспечение дисциплины

1) Рекомендуемая литература

а) Основная литература

Богульская, Н. А. Модели безопасности компьютерных систем : учебное пособие / Н. А. Богульская, М. М. Кучеров. — Красноярск : СФУ, 2019. — 206 с. — ISBN 978-5-7638-4008-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157578

Пушкарёв, В. В. Защита информационных процессов в компьютерных системах : учебное пособие / В. В. Пушкарёв, В. П. Пушкарёв. — Москва : ТУСУР, 2012. — 131 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/4925

Информационная безопасность и защита информации: Учебное пособие. / Баранова Е.К., Бабаш А.В. — 3-е изд., перераб. и доп. — М.: РИОР: ИНФРА-М, 2017. — 322 с. — (Высшее образование). [Электронный ресурс]. – Режим доступа: http://znanium.com/go.php?id=763644

б) Дополнительная литература:

Щербаков, А. Современная компьютерная безопасность. Теоретические основы. Практические аспекты : учебное пособие / А. Щербаков. – Москва : Книжный мир, 2009. – 352 с. – (Высшая школа). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=89798

Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс]/ А.А. Петров.— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 446 с.— Режим доступа: http://www.iprbookshop.ru/63800.html

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 02.08.2023г.
6. https://cyberleninka.ru/ научная электронная библиотека «Киберленинка».

7. Научная электронная библиотека eLIBRARY.RU (подписка на журналы) https://elibrary.ru/projects/subscription/rus_titles_open.asp;

8. Репозитарий ТвГУ http://eprints.tversu.ru

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

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

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

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.	Набор учебной мебели, меловая доска, Переносной ноутбук, Интерактивная система Smart Board 660iv со встроенным проектором	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 224, 170002, г.Тверь, Садовый пер-к, д. 35	Набор учебной мебели, меловая доска, Переносной ноутбук, Мультимедийный проектор BenQ MP 724 с потолочным креплением и экраном 1105	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.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Обновление списка литературы.	Протокол № 11 от 26.06.2013
2.	VII. Методические указания для обучающихся по освоению дисциплины	Корректировка планов практических (семинарских) занятий и методических рекомендаций к ним.	Протокол № 10 от 24.06.2014
3.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Обновление списка литературы. Обновление ссылок из ЭБС.	Протокол № 1 от 27.09.2015
4.	VII. Методические указания для обучающихся по освоению дисциплины.	Корректировка планов практических (семинарских) занятий и методических рекомендаций к ним.	Протокол № 1 от 01.09.2016
5.	I - X	Корректировка всех разделов в соответствии с новым стандартом	Протокол № 6 от 28.02.2017
6.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Дополнение списков. Обновление ссылок из ЭБС.	Протокол № 1 от 01.09.2018
7.	I - VIII	Корректировка всех разделов в соответствии с новым стандартом	Протокол № 10 от 29.06.2021

8.	V. Учебно-методическое и информационное обеспечение дисциплины	Обновление списков ПО. Обновление ссылок из ЭБС.	Протокол № 1 от 1.09.2023
9.	II. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий, IV. Оценочные материалы для проведения текущей и промежуточной аттестации	Корректировка наименований разделов и тем. Корректировка оценочных материалов	Протокол № 7 от 7.03.2024