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

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

Рабочая программа дисциплины (с аннотацией)

Основы информационной безопасности

Специальность

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»

Для студентов очной формы обучения

СПЕЦИАЛИТЕТ

Для студентов 2 курса ОФО

Составитель:
Чернышев О. Я.

Тверь 2023

I. Аннотация

1. Цель и задачи дисциплины

Дисциплина «Основы информационной безопасности» имеет цель - раскрыть содержание основных понятий и формальных моделей обеспечения безопасности компьютерных систем (моделей информационной безопасности).

Задачами освоения дисциплины являются:

1) получение базовых знаний и понятий в сфере компьютерной безопасности;

2) получение теоретических знаний о методологии анализа архитектурных (схемно-технических) и программно-алгоритмических решений, применяемых в системах защиты информации современных компьютерных систем;

3) изучение общих принципов, анализа и обоснования моделей, методов и механизмов обеспечения компьютерной безопасности.

2. Место дисциплины в структуре ООП

Данная дисциплина входит в обязательную часть учебного плана, связана с другими дисциплинами образовательной программы: «Введение в специальность», «Безопасность жизнедеятельности».

Дисциплины, для которых освоение данной дисциплины необходимо как предшествующее: «Техническая защита информации», «Модели безопасности компьютерных систем», «Организационное и правовое обеспечение информационной безопасности».

3. Объем дисциплины: 3 зачетные единицы, 108 академических часов, в том числе:

контактная аудиторная работа: лекции – 36 часов, в т.ч. практическая подготовка – 0 часов;

самостоятельная работа: 72 часа.

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-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	**ОПК-1.1** Определяет угрозы информационной безопасности для объекта информатизации
	ОПК-1.2 Осуществляет классификацию защищаемой информации по видам тайны и степеням конфиденциальности
	ОПК-1.3 Применяет основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	**ОПК-5.1** Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности

5. Форма промежуточной аттестации и семестр прохождения – зачет в 4 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. Основные понятия компьютерной безопасности	25	8	0	0	17
Раздел 2. Систематика методов и механизмов обеспечения компьютерной безопасности	42	14	0	0	28
Раздел 3. Угрозы безопасности в компьютерных системах	41	14	0	0	31
ИТОГО	108	36	0	0	72

III. Образовательные технологии

Учебная программа – наименование разделов и тем	Вид занятия	Образовательные технологии
Раздел 1. Основные понятия компьютерной безопасности	лекция практическое	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция.

Раздел 2. Систематика методов и механизмов обеспечения компьютерной безопасности	лекция практическое	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция, кейс-технология, технология развития креативного мышления
Раздел 3. Угрозы безопасности в компьютерных системах	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-1.1, ОПК-1.2): Для КС ТвГУ определить требования к защите информации

Раздел II.

Задание 1 (ОПК-5.1): Опишите порядок засекречивания информации, составляющей государственную тайну

Раздел III.

Задание 1 (ОПК-1.3): Постройте концептуальную модель безопасности информации.

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

Проверяемые индикаторы достижения компетенций: ОПК-1.1; ОПК-1.2; ОПК-1.3; ОПК-5.1

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

Примерные вопросы к зачету

1. Основные документы, определяющие концептуальные основы информационной безопасности РФ.
2. Концепция национальной безопасности РФ. Важнейшие задачи обеспечения национальной безопасности в информационной сфере.
3. Доктрина информационной безопасности.
4. Понятие угрозы информации. Угрозы конфиденциальности, целостности и доступности.
5. Классификация угроз информации.
6. Модель действий нарушителя.
7. Источники угроз информационной безопасности РФ. Внешние источники угроз.

8. Источники угроз информационной безопасности РФ. Внутренние источники угроз. Причины и источники угроз национальным интересам страны.
9. Виды безопасности.
10.Национальная безопасность и её составляющие.
11.Субъекты системы и уровни обеспечения национальной безопасности РФ.
12.Основные задачи по обеспечению национальной безопасности.
13.Понятие информационной войны. Проблемы информационных войн.
14.Субъекты и цели информационного противоборства. Составные части и методы информационного противоборства.
15. Информационное оружие, его классификация и возможности.
16. Информационная война как целенаправленное информационное воздействие информационных систем.
17.Приемы информационного воздействия в информационной войне. Способы перепрограммирования информационных систем.
18.Типовая стратегия информационной войны. Основные аспекты и последствия информационной войны.
19.Информационное оружие, его классификация и возможности.
20.Методы нарушения конфиденциальности, целостности и доступности информации.
21.Причины, виды, каналы утечки и искажения информации.
22.Основные направления обеспечения информационной безопасности объектов информационной сферы.
23.Методы и средства обеспечения ИБ объектов информационной сферы.
24.Стандарты и нормативы в сфере обеспечения информационной безопасности.
25.Определение безопасности компьютерной системы и категории требований безопасности.
26.Базовые требования безопасности компьютерной системы.
27.Классы безопасности компьютерных систем, понятие риска.
28.Режимы функционирования компьютерной системы.
29.Правила разграничения доступа к информации. Мандатная модель управления доступом.
30.Правила разграничения доступа к информации. Дискреционная модель управления доступом.
31.Основные понятия криптографической защиты информации. Историческая справка об основных этапах развития криптографии как науки.
32.Основные требования к криптографическим системам защиты информации. Пример простейшего шифра.
33.Обобщенная схема симметричной криптосистемы. Стандарт шифрования ГОСТ 28147-89. Особенности применения алгоритмов симметричного шифрования.
34. Сущность понятий: идентификация, аутентификация; авторизация.
35.Пароли, сертификаты и цифровые подписи. Методы аутентификации.

36.Понятие разграничения доступа. Разграничение доступа по виду, характеру, назначению, степени важности и секретности информации.

37.Технология межсетевых экранов (МЭ). Виды МЭ.

38.Технология межсетевых экранов (МЭ). Функции МЭ.

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

Нестеров С. А. Основы информационной безопасности [Электронный ресурс] : учебник для вузов / С. А. Нестеров. - 2-е изд., стер. - Санкт-Петербург : Лань, 2023. - 324 с. – Режим доступа: https://e.lanbook.com/book/341267

Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс] : учебник для вузов / О. В. Прохорова. - 5-е изд., стер. - Санкт-Петербург : Лань, 2023. - 124 с. – Режим доступа: https://e.lanbook.com/book/293009

Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций: учебное пособие / Ю.Н. Загинайлов. - М.; Берлин: Директ-Медиа, 2015. - 105 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3947-4 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=362895

б) Дополнительная литература:

Сычев Ю.Н. Основы информационной безопасности [Электронный ресурс]: учебное пособие /Ю.Н. Сычев.— Электрон. текстовые данные.— М.: Евразийский

открытый институт, 2010.— 328 с.— Режим доступа: http://www.iprbookshop.ru/10746.html

Клименко И. С. Информационная безопасность и защита информации: модели и методы управления : Монография / И. С. Клименко; Северо-Кавказский федеральный университет, ф-л в г. Пятигорске. - 1. - Москва : ООО "Научно-издательский центр ИНФРА-М", 2024. - 180 с. - (Научная мысль). – Режим доступа: https://znanium.com/catalog/document?id=431346

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)

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 100 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	50	18	12	20
2	50	18	12	20

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**

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, Учебная аудитория № 314 (Корпус 3, 170002, Тверская обл., г.Тверь, пер. Садовый, дом 35)	Набор учебной мебели, меловая доска, Мультимедийный комплект учебного класса	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	Описание внесенных изменений	Реквизиты документа, утвердившего изменения
1.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Обновление списка литературы. Обновление ссылок из ЭБС.	Протокол № 1 от 27.09.2015
2.	VII. Методические указания для обучающихся по освоению дисциплины.	Корректировка планов практических (семинарских) занятий и методических рекомендаций к ним.	Протокол № 1 от 01.09.2016
3.	I - X	Корректировка всех разделов в соответствии с новым стандартом	Протокол № 6 от 28.02.2017
4.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Дополнение списков. Обновление ссылок из ЭБС.	Протокол № 1 от 01.09.2017

5.	I - VIII	Корректировка всех разделов в соответствии с новым стандартом	Протокол № 10 от 29.06.2021
6.	V. Учебно-методическое и информационное обеспечение дисциплины	Обновление списков ПО. Обновление ссылок из ЭБС.	Протокол № 1 от 1.09.2023