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)

Основы информационной безопасности

Специальность
10.05.01 Компьютерная безопасность

Специализация
Математические методы защиты информации

Для студентов 2 курса очной формы обучения

Составитель: к.т.н. П.В. Кратович

Тверь 2023

I. Аннотация

1. Наименование дисциплины (или модуля) в соответствии с учебным планом

Основы информационной безопасности

2. Цель и задачи дисциплины (или модуля)

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

Задачи дисциплины - дать основы:

- исходных понятий и формализации в сфере компьютерной безопасности;
- представления, анализа и обоснования моделей, методов и механизмов обеспечения компьютерной безопасности;
- методологии анализа архитектурных (схемно-технических) и программно-алгоритмических решений, применяемых в системах защиты информации современных компьютерных систем.

3. Место дисциплины (или модуля) в структуре ООП

Данная дисциплина является учебной дисциплиной базовой части учебного плана специальности «Компьютерная безопасность», и призвана сформировать у обучаемых теоретико-методологические основы профессиональной деятельности в сфере компьютерной безопасности в контексте всех трех ее составляющих видов - производственно-технологической, организационно-управленческой и экспериментально-исследовательской.

Знания и умения, приобретенные в ходе изучения дисциплины «Основы информационной безопасности» используются студентами при изучении всех остальных общепрофессиональных дисциплин и дисциплин специализации в рамках учебного плана специальности «Компьютерная безопасность».

4. Объем дисциплины (или модуля):

3 зачетных единиц, 108 академических часов, **в том числе**

контактная работа: лекции 36 часов, **самостоятельная работа:** 72 часа.

5. Перечень планируемых результатов обучения по дисциплине (или модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	Планируемые результаты обучения по дисциплине (или модулю)
ОПК-4 – способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	**Владеть:** современными методами научных исследований в профессиональной деятельности. **Уметь:** обрабатывать, анализировать и систематизировать результаты выполненных научных исследований, систематизировать и обобщать результаты анализа научно-технической информации, **Знать:** методы теории вероятностей, теории случайных процессов и математической статистики, методологические основы информационно-аналитической деятельности, методы апробации и внедрения результатов научных исследований, научные методы и средства оценки эффективности технологий автоматизации информационно-аналитической деятельности.
ПК-10 – способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы	**Владеть:** основными методами и средствами ведения информационных противоборств. **Уметь:** применять методологию анализа архитектурных (схемно-технических) и программно-алгоритмических решений в системах защиты информации современных компьютерных систем. **Знать:** основные принципы, методы и механизмы обеспечения безопасности объектов информатизации.

антивирусной защиты, средства криптографической защиты информации	

6. Форма промежуточной аттестации зачет

7. Язык преподавания русский**.**

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

1. **Для студентов очной формы обучения набора 2017 г.**

Учебная программа – наименование разделов и тем	Всего (час.)	Контактная работа (час.)		Самостоятельная работа и контроль (час.)
		Лекции	Практические (лабораторные) занятия	
Раздел 1. Основные понятия компьютерной безопасности	27	9		18
Раздел 2. Систематика методов и механизмов обеспечения компьютерной безопасности	42	14		28
Раздел 3. Угрозы безопасности в компьютерных системах	39	13		26
ИТОГО	108	36		72

III. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (или модулю)

Методические рекомендации по организации самостоятельной работы студентов

Планы практических (семинарских) занятий и методические рекомендации к ним

IV. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (или модулю)

Типовые контрольные задания для проверки уровня сформированности компетенций ОПК-4, ПК-10

Этап формирования компетенции, в котором участвует дисциплина	**Типовые контрольные задания для оценки знаний, умений, навыков (2-3 примера)**	**Показатели и критерии оценивания компетенции, шкала оценивания**
базовый **владеть**	**1.** Для КС ТвГУ описать объект защиты. **2.** Для КС ТвГУ определить виды угроз и характер происхождения угроз. **3.** Для КС ТвГУ определить требования к защите информации.	Имеется полное верное решение, включающее правильный ответ – 3 балла Решение не дано или дано неверное решение – 0 баллов
базовый **уметь**	**1.** Постройте концептуальную модель безопасности информации. **2.** Опишите порядок засекречивания информации, составляющей государственную тайну.	Имеется полное верное решение, включающее правильный ответ – 3 балла Решение не дано или дано неверное решение – 0 баллов
базовый **знать**	**1.** Система правовых, организационных, технических и иных мер, федеральных органов власти, местного самоуправления, предприятий, организаций и учреждений, направленных на обеспечение безопасности Российской Федерации, сохранения ее государственной, служебной, коммерческой, других видов тайн и сведений ограниченного доступа, информационных ресурсов, систем, технологий и средств их обеспечения, называется: *a. Системой информационной безопасности.* *b. Доктриной информационной безопасности.* *c. Государственной системой*	Имеется полное верное решение, включающее правильный ответ – 3 балла Решение не дано или дано неверное решение – 0 баллов

	защиты информации. *d. Режимом секретности.* **2.** Какой орган при осуществлении своей деятельности имеет право подготавливать и представлять в установленном порядке Президенту и в Правительство РФ предложения по правовому регулированию вопросов защиты государственной тайны, совершенствованию системы защиты государственной тайны? *a. Государственная техническая комиссия при Президенте РФ.* *b. Межведомственная комиссия по защите государственной тайны.* *c. Федеральная служба безопасности России.* *d. Федеральное агентство правительственной связи и информации.* **3.** Защита персональных данных, страхование информации и информационных систем осуществляется: *a. Комплексной системой информационной безопасности.* *b. Организационно-правовой системой защиты информации.* *c. Государственной системой организационно-правового обеспечения информационной безопасности.* d. *Организационно-функциональной системой защиты информации.*	

V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (или модуля)

а) Основная литература:

1. 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

2. Сычев, Ю. Н. **Основы информационной безопасности** : учебно-практическое пособие : [16+] / Ю. Н. Сычев. – Москва : Евразийский открытый институт, 2010. – 328 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=90790

б) Дополнительная литература

1. Галатенко, В. А. **Основы информационной безопасности** : Курс лекций : учебное пособие / В. А. Галатенко ; под ред. В. Б. Бетелина. – Изд. 3-е. – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2006. – 208 с. – (**Основы** информационных технологий). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=233063

2. Гультяева, Т. А. **Основы информационной безопасности** : учебное пособие : [16+] / Т. А. Гультяева. – Новосибирск : Новосибирский государственный технический университет, 2018. – 79 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574729

VI. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (или модуля)

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.

VII. Методические указания для обучающихся по освоению дисциплины

Методические рекомендации по организации самостоятельной работы студентов

Самостоятельная работа студентов по изучаемой дисциплине призвана, не только, закреплять знания, полученные во время аудиторных занятий, но и способствовать развитию у студентов творческих навыков, инициативы, умению организовывать свое время.

Все виды самостоятельной работы и планируемые на их выполнение затраты времени в часах исходят из того, что студент достаточно активно работал в аудитории, слушая лекции и решая задачи на практических занятиях. В случае пропуска лекций и практических занятий студенту потребуется сверхнормативное время на освоение пропущенного материала.

При выполнении плана самостоятельной работы студенту необходимо прочитать теоретический материал, содержащийся в указанной учебной литературе и Интернет-ресурсах.

Планы практических (семинарских) занятий

Раздел 1. Основные понятия компьютерной безопасности

История развития теории и практики обеспечения компьютерной безопасности.

Понятия «информационная безопасность» и компьютерная безопасность. Безопасность информации в компьютерных системах и ее составляющие - конфиденциальность, целостность и правомерная доступность (сохранность) информации.

Субъекты и объекты безопасности. Угрозы безопасности. Нарушители безопасности.

Общие принципы обеспечения компьютерной безопасности.

Раздел 2. Систематика методов и механизмов обеспечения компьютерной безопасности.

Методы и механизмы, непосредственно обеспечивающие конфиденциальность, целостность и доступность информации - разграничение

доступа к данным, контроль, управления информационной структурой данных, установление и контроль ограничений целостности данных, шифрование данных, механизмы ЭЦП данных в процессах их передачи и хранения, защита/удаление остаточной информации на носителях данных и в освобождаемых областях оперативной памяти.

Методы и механизмы общеархитектурного характера - идентификация/аутентификация пользователей, устройств, данных, управление памятью, потоками, изоляция процессов, управление транзакциями.

Методы и механизмы инфраструктурного характера - управление (контроль) конфигурацией, управление сеансами, управление удаленным доступом с рабочих станций, управление сетевым соединениями, управление инфраструктурой сертификатов криптоключей.

Методы и механизмы обеспечивающего (профилактирующего) характера - протоколирование и аудит событий, резервирование данных, журнализация процессов изменения данных, профилактика, учет и контроль использования носителей данных, нормативно-организационная регламентация использования КС, обучение, нормативно-административное побуждение и принуждение пользователей по вопросам информационной безопасности КС.

Раздел 3. Угрозы безопасности в компьютерных системах

Понятие угрозы. Угрозы безопасности информации в компьютерных системах.

Понятия «идентификация», «аутентификация», «авторизация», «спецификация», «классификация», «категорирование» и «каталогизация».

Классификационные схемы (каталогизация) угроз. Теоретические (формальные) основы классификации - критерии выделения и таксономия классов (алгебраическая полнота в операциях пересечения и объединения классов).

Примеры и проблемы теоретического обоснования каталогов угроз по зарубежным, отечественным и международным стандартам.

Идентификация и спецификация (описание) угроз - выявление угрозы определенного типа и присвоение ей уникального идентификатора, определение и описания источника (природы) угрозы, активов/объектов, подверженных воздействию угрозы, способов и особенностей реализации/осуществления.

Общая схема оценивания угроз - оценка [вероятности] реализации угрозы и оценка ущерба от реализации угрозы. Оценка рисков, методы и шкалы оценки. Методы экспертной оценки вероятности реализации и/или степени опасности угроз.

Человеческий фактор в угрозах безопасности и модель нарушителя информационной безопасности.

Требования к рейтинг-контролю.

Модуль 1.

Максимальная сумма баллов по модулю – 50, из них 30 баллов отводится на текущий контроль учебной работы студента, 20 баллов на рубежный контроль по модулю. Текущая работа студента складывается из ответов в аудитории (min – 0 баллов, max - 3 балла). Рубежный контроль проводится в форме контрольной работы.

Модуль 2.

Максимальная сумма баллов по модулю – 50, из них 30 баллов отводится на текущий контроль учебной работы студента, 20 баллов на рубежный контроль по модулю. Текущая работа студента складывается из ответов в аудитории (min – 0 баллов, max – 3 балла). Рубежный контроль проводится в форме контрольной работы.

Вопросы для подготовки 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. Обобщенная схема асимметричной криптосистемы шифрования с открытым ключом. Функция хэширования.
35. Обобщенная схема асимметричной криптосистемы шифрования с открытым ключом. Электронная подпись.
36. Сущность понятий: идентификация, аутентификация; авторизация.
37. Пароли, сертификаты и цифровые подписи. Методы аутентификации.
38. Понятие разграничения доступа. Разграничение доступа по виду, характеру, назначению, степени важности и секретности информации.

39. Технология межсетевых экранов (МЭ). Виды МЭ.
40. Технология межсетевых экранов (МЭ). Функции МЭ.

VIII. Перечень педагогических и информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (по необходимости)

Преподавание учебной дисциплины строится на сочетании лекций, практических занятий и различных форм самостоятельной работы студентов.

Программное обеспечение:

Наименование 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)	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, Учебная аудитория № 224 (Корпус 3, 170002, Тверская обл., г.Тверь, пер. Садовый, дом 35)	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, Учебная аудитория № 203 (Корпус 3, 170002, Тверская обл., г.Тверь, пер.	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

Садовый, дом 35)	

IX. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Наименование специальных* помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений 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, Учебная аудитория № 314 (Корпус 3, 170002, Тверская обл., г.Тверь, пер. Садовый, дом 35)	Набор учебной мебели, меловая доска, Мультимедийный комплект учебного класса (вариант № 2): Проектор Casio XJ-140 настенный проекц. экран Lumien 180*180, Ноутбук Dell N4050, сумка 15,6", мышь; Усилитель Roxton AA-120; Радиосистема Shure PG288/PG58; Микшер Mackie 402 VLZ; Стационарный микрофон SOUNDKING EG002 с настольным держателем; Мультимедийный проектор Casio XJ-H2650 с потолочным креплением и мотириз. экраном; Шкаф напольный 19".
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 № 224 (Корпус 3, 170002, Тверская обл., г.Тверь, пер. Садовый, дом 35)	Набор учебной мебели, меловая доска, Переносной ноутбук, Мультимедийный проектор BenQ MP 724 с потолочным креплением и экраном 1105
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 № 203 (Корпус 3, 170002, Тверская обл., г.Тверь, пер. Садовый, дом 35)	Набор учебной мебели, меловая доска, Переносной ноутбук, Интерактивная система Smart Board 660iv со встроенным проектором

X. Сведения об обновлении рабочей программы дисциплины (или модуля)

№п. п.	**Обновленный раздел рабочей программы дисциплины**	**Описание внесенных изменений**	**Дата и протокол заседания кафедры, утвердившего**

	(или модуля)		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.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Дополнение списков. Обновление ссылок из ЭБС.	Протокол № 1 от 01.09.2023