Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Тверской государственный университет»

Утверждаю:

Руководитель ООП:

_____ Н.А. Семыкина

«_9_» _06_ 2023 г.

Рабочая программа дисциплины (с аннотацией)

Введение в специальность

Специальность
10.05.01 Компьютерная безопасность

Специализация
Математические методы защиты информации

Для студентов 1 курса

Форма обучения
Очная

Составитель: доцент, к.ф.м.н. Ю.В. Чемарина

Тверь 2023

I. Аннотация

1. Наименование дисциплины в соответствии с учебным планом

Введение в специальность

2. Цель и задачи дисциплины

Целью освоения дисциплины является изучение материала, относящегося к общим основам математических методов защиты информации в профессиональной деятельности:

1) формирование системных основ использования математического аппарата будущими специалистами в предметной области;
2) формирование умений осознано применять инструментальные средства информационных технологий для защиты информации;
3) формирование навыков к самообучению и непрерывному профессиональному самосовершенствованию.

Задачами освоения дисциплины являются:

1) усвоение основных понятий теории защиты информации;
2) систематизация знаний по защищенными компьютерными системам и средствам обработки, хранения и передачи информации; службам защиты информации; математическим моделям процессов, возникающих при защите информации.

3. Место дисциплины в структуре ООП

Дисциплина входит в базовую часть ООП «Компьютерная безопасность».

Изучение дисциплины основывается на базовых знаниях студентов, приобретенных в рамках школьного курса «Информатика и ИКТ».

Требования к начальному уровню подготовки студента, необходимому для успешного освоения дисциплины не выходят за рамки школьных курсов «Информатика и ИКТ», «Математика».

Дисциплина «Введение в специальность» формирует у студента умения и навыки, которые будут в дальнейшем использоваться при изучении следующих дисциплин: «Основы информационной безопасности», «Модели безопасности

компьютерных систем», «Криптографические методы защиты информации», «Математические методы оценки защищенности компьютерных систем», «Организационное и правовое обеспечение информационной безопасности».

4. Объем дисциплины:

6 зачетных единиц, 216 академических часов, **в том числе**

контактная работа: лекции 0 часов, практические занятия 72 часа, **самостоятельная работа:** 144 часов.

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

Планируемые результаты освоения образовательной программы (формируемые компетенции)	**Планируемые результаты обучения по дисциплине**
Базовый уровень ОК-5. Способность понимать социальную значимость своей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	**Владеть:** навыками подбора нормативных и методических материалов по вопросам обеспечения информационной безопасности. **Уметь:** применять современные технологии для обеспечения информационной безопасности. **Знать:** основы современных технологий обеспечения информационной безопасности и защиты интересов личности, общества и государства.
Базовый уровень ПК-7. Способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем	**Владеть:** современными методами анализа проектных решений в области защиты компьютерных систем. **Уметь:** проводить анализ проектных решений в области защиты компьютерных систем. **Знать:** современные требования к проектным

	решениям по обеспечению защищенности компьютерных систем.
Базовый уровень ПК-19. Способность производить проверки технического состояния и профилактические осмотры технических средств защиты информации	**Владеть:** необходимыми техническими знаниями и практическими навыками работы со средствами защиты информации..
	Уметь: производить проверки технического состояния и профилактические осмотры технических средств защиты информации.
	Знать: технические характеристики и инструментарий средств защиты информации.
Базовый уровень ПК-20. Способность выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций	**Владеть:** необходимыми техническими знаниями и практическими навыками работы со средствами защиты информации.
	Уметь: выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций.
	Знать: технические характеристики и режимы работы средств защиты информации, возможные нештатные ситуации.

6. Форма промежуточной аттестации:

экзамен.

7. Язык преподавания: русский**.**

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

Для студентов очной формы обучения

Наименование разделов и тем	Всего (час.)	Контактная работа (час.)		Самостоятельная работа (час.)
		Лекции	Практические работы	
Основы защиты информации	54	0	18	36

Технические и программные средства защиты информации	54	0	18	36
Правовое законодательство в сфере информационной безопасности	54	0	18	36
Математические методы защиты информации	54	0	18	36
ИТОГО	216	0	72	144

III. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Основу самостоятельной работы студента составляют: усвоение теоретического материала, чтение учебной литературы, выполнение домашних работ, подготовка рефератов и решение дополнительных задач, способствующих развитию практических навыков применения математических методов защиты информации.

Тематика рефератов и методические рекомендации по их написанию:

Требования к оформлению рефератов и докладов

Процесс работы лучше разбить на следующие этапы:

- Определить и выделить проблему.
- На основе первоисточников самостоятельно изучить проблему.
- Провести обзор выбранной литературы.
- Логично изложить материал.

Объектами внимания автора должны стать следующие составляющие структуры будущей работы:

1) титульный лист,

2) оглавление (содержание),

3) текст (введение, основная часть, заключение),

4) ссылки (сноски или примечания),

5) цитаты,

6) список литературы.

Во введении излагается цель и задачи работы, обоснование выбора темы и её актуальность. Объём: 1—2 страницы.

Основная часть содержит точку зрения автора на основе анализа литературы по проблеме. Объём: 12—15 страниц.

В заключении формируются выводы и предложения. Заключение должно быть кратким, четким, выводы должны вытекать из содержания основной части. Объём: 1—3 страницы.

Список используемой литературы.

В реферате могут быть приложения в виде схем, анкет, диаграмм и прочего. В оформлении реферата приветствуются рисунки и таблицы.

Темы для рефератов

1. Место и роль информационной безопасности в различных сферах жизнедеятельности личности (общества, государства).

2. Правовая база обеспечения информационной безопасности личности (общества, государства).

3. Виды защищаемой информации.

4. Интересы личности (общества, государства) в информационной сфере.

5. Угрозы информационной безопасности Российской Федерации.

6. Внешние (внутренние) источники угроз информационной безопасности государства.

7. Проблемы региональной информационной безопасности.

8. Информационное оружие, его классификация и возможности.

9. Методы нарушения конфиденциальности (целостности, доступности) информации.

10.Правовые (организационно-технические, экономические) методы обеспечения информационной безопасности.

11.Компьютерная система как объект информационной безопасности.

12.Обеспечение информационной безопасности компьютерных систем.

18.Субъекты информационного противоборства.

19.Цели информационного противоборства.

20.Составные части и методы информационного противоборства.

21.Информационное оружие, его классификация и возможности.

22.Методы нарушения конфиденциальности, целостности и доступности информации.

23.Причины, виды, каналы утечки и искажения информации.

24.Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.

25.Правовые, организационно-технические и экономические методы обеспечения информационной безопасности.

26.Модели, стратегии и системы обеспечения информационной безопасности.

27.Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.

28.Компьютерная система как объект информационной безопасности.

29.Общая характеристика методов и средств защиты информации.

30.Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности.

31.Программно-аппаратные средства обеспечения информационной безопасности.

IV. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

1. Типовые контрольные задания для проверки уровня сформированности компетенции

Этап формирования компетенции, в	Типовые контрольные задания для оценки знаний, умений, навыков (2-3 примера)	Показатели и критерии оценивания

котором участвует дисциплина		компетенции, шкала оценивания
базовый **владеть**	1. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации называется… Выберите один из 4 вариантов ответа: 1) кодируемой 2) шифруемой 3) недостоверной 4) защищаемой. 2. Какие законы существуют в России в области компьютерного права? Выберите несколько из 6 вариантов ответа: 1) О государственной тайне 2) об авторском праве и смежных правах 3) о гражданском долге 4) о правовой охране программ для ЭВМ и БД 5) о правовой ответственности 6) об информации, информатизации, защищенности информации.	• Правильно выбран вариант ответа – 1 балл
базовый **уметь**	1. Как настроить длину пароля? Почему необходимо ограничивать нижнее значение длины пароля? 2. Как проверить установленные параметры политики паролей? 3. Какие дополнительные параметры политики учетных записей можно настроить? Как это сделать? 4. Как настроить политику	• Дан верный полный ответ – 3 балла • Дан верный, но недостаточно полный ответ – 2 балла • Представлены отдельные верные рассуждения, относящиеся к вопросу – 1 балл

	блокировки учетной записи? В каком случае это бывает нужно?	• Ответ не дан ИЛИ дан неверный ответ – 0 баллов
базовый **знать**	1. Утечка информации – это… Выберите один из 3 вариантов ответа: 1) несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу; 2) ознакомление постороннего лица с содержанием секретной информации; 3) потеря, хищение, разрушение или неполучение переданных данных. 2. Выделите группы, на которые делятся средства защиты информации: Выберите один из 3 вариантов ответа: 1) физические, аппаратные, программные, криптографические, комбинированные; 2) химические, аппаратные, программные, криптографические, комбинированные; 3) физические, аппаратные, программные, этнографические, комбинированные.	• Правильно выбран вариант ответа – 1 балл

Перечень вопросов для проведения экзамена

1. Основные понятия защиты информации (субъекты, объекты, доступ, граф доступов, информационные потоки).

2. Постановка задачи построения защищенной автоматизированной системы (АС). Модели ценности информации.
3. Угрозы безопасности информации. Угрозы конфиденциальности, целостности, доступности, раскрытия параметров АС.
4. Понятие политики безопасности. Дискреционная политика безопасности. Мандатная политика безопасности. Мандатная политика целостности.
5. Модель системы безопасности HRU. Основные положения модели.
6. Основные положения Руководящих документов ГТК в области защиты информации.
7. Определение и классификация НСД. Определение и классификация нарушителя. Классы защищенности АС от НСД к информации.
8. Фундаментальные требования компьютерной безопасности. Требования классов защиты.
9. Криптосистемы с открытым ключом.
10. Понятие сертификата. Криптосистема RSA. Выбор параметров.
11. Стандарты ГОСТ Р 34.11 и SHA.
12. Цифровая подпись. Схемы цифровой подписи.
13. Стандарты ГОСТ Р 34.10 и DSS.
14. Структура и состав системы нормативных правовых актов, регулирующих обеспечение информационной безопасности в РФ.
15. Правовой режим защиты государственной тайны.
16. Организация и обеспечение режима секретности.
17. Лицензирование и сертификация в области защиты информации.
18. Правовые основы защиты информации с использованием технических средств.

V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) Основная литература

1. Информационная безопасность и защита информации: учеб. пособие / Баранова Е.К., Бабаш А.В. —3-е изд., перераб. и доп. —М. : РИОР :

ИНФРА-М, 2017. —322 с. —(Высшее образование). — ww.dx.doi.org/10.12737/11380. -Режим доступа: http://znanium.com/catalog/product/763644

2. Черпаков И. В. Теоретические основы информатики : учебник и практикум для вузов / И. В. Черпаков - Электрон. дан. - Москва : Юрайт, 2022. - 353 с. - (Высшее образование). - URL: https://urait.ru/bcode/487320

б) Дополнительная литература:

1. Хорев П. Б. Программно-аппаратная защита информации : учебное пособие / П. Б. Хорев; Московский энергетический институт. - 3. - Москва : ООО "Научно-издательский центр ИНФРА-М", 2022. - 327 с. - (Высшее образование: Магистратура). - ВО - Бакалавриат. – Режим доступа: https://znanium.com/catalog/document?id=397282
2. Жук А. П. Защита информации : учебное пособие / А. П. Жук, Е. П. Жук; Северо-Кавказский федеральный университет. - 3. - Москва : Издательский Центр РИОР, 2021. - 400 с. - Профессиональное образование. Режим доступа : http://znanium.com/catalog/document?id=367588
3. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шаньгин; Московский институт электронной техники. - 1. - Москва : Издательский Дом "ФОРУМ", 2022. - 592 с. - (Высшее образование: Бакалавриат). - ВО - Бакалавриат. – Режим доступа: https://znanium.com/catalog/document?id=389857
4. Бабаш А. В. История защиты информации в зарубежных странах : Учебное пособие / А. В. Бабаш, Д. А. Ларин; Национальный исследовательский университет "Высшая школа экономики"; Национальный исследовательский университет "Высшая школа экономики". - 1. - Москва : Издательский Центр РИОР, 2021. - 284 с. - (Высшее образование: Бакалавриат). - ВО - Бакалавриат. – Режим доступа: https://znanium.com/catalog/document?id=368004
5. Бабаш А. В. Моделирование системы защиты информации: практикум : учебное пособие / А. В. Бабаш, Е. К. Баранова; Национальный исследовательский университет "Высшая школа экономики". - 3. - Москва : Издательский Центр РИОР, 2021. - 320 с. - (Высшее образование: Бакалавриат). - ВО - Бакалавриат. – Режим доступа: https://znanium.com/catalog/document?id=371348.

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

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.

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
9.Справочно-правовая система «Консультант Плюс» www.consultant.ru;
10. Справочно-правовая система «Гарант» » www.garant.ru.

VII. Методические указания для обучающихся по освоению дисциплины

Подготовка к практическим занятиям по дисциплине включает в себя:

- изучение теоретического материала, необходимого для решения практических задач;
- решение практических задач;
- подготовку к контрольным работам;
- подготовку докладов.

Темы докладов

1. Понятие национальной безопасности.

2. Виды безопасности и сферы жизнедеятельности личности, общества и государства.

3. Виды защищаемой информации.

4. Основные понятия и общеметодологические принципы теории информационной безопасности.

5. Роль информационной безопасности в обеспечении национальной безопасности государства.

6. Интересы личности в информационной сфере.

7. Интересы общества в информационной сфере.

8. Интересы государства в информационной сфере.

9. Основные составляющие национальных интересов Российской Федерации в информационной сфере.

10.Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России.

11.Угрозы информационному обеспечению государственной политики Российской Федерации.

12.Угрозы развитию отечественной индустрии информации, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов.

13.Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

14.Внешние источники угроз.

15.Внутренние источники угроз.

16.Направления обеспечения информационной безопасности.

Требования к рейтинг-контролю: учебный материал разбивается на 2 модуля.

1 модуль

Вид контроля	**Формы контроля**	**Максимальный балл**
Текущий контроль	домашние работы	5
	активность на занятиях	5
	посещаемость	5
Рубежный контроль	контрольная работа №1	15
Общая сумма баллов:		30

2 модуль

Вид контроля	Формы контроля	Максимальный балл
Текущий контроль	домашние работы	5
	активность на занятиях	5
	посещаемость	5
Рубежный контроль	контрольная работа №2	15
Общая сумма баллов:		30

Рейтинг студента складывается из баллов, полученных по каждому модулю. Максимальная сумма баллов за семестр – 60. Максимальная сумма баллов за экзамен – 40.

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

В процессе освоения дисциплины используются следующие образовательные технологии, способы и методы формирования компетенций: практическое занятие, упражнения, подготовка письменных аналитических работ, подготовка рефератов и докладов.

Наряду с традиционными образовательными технологиями используются проектные и исследовательские технологии, в результате чего студент может овладеть навыками компьютерного самообучения и математического моделирования.

Adobe Acrobat Reader DC - Russian	бесплатно
Cadence SPB/OrCAD 16.6	Государственный контракт на поставку лицензионных программных продуктов 103 - ГК/09 от 15.06.2009
Git version 2.5.2.2	бесплатно
Google Chrome	бесплатно
Kaspersky Endpoint Security 10 для Windows	Акт на передачу прав ПК545 от 16.12.2022
Lazarus 1.4.0	бесплатно
Mathcad 15 M010	Акт предоставления прав ИС00000027 от 16.09.2011;
MATLAB R2012b	Акт предоставления прав № Us000311 от 25.09.2012;

Многофункциональный редактор ONLYOFFICE	бесплатно
ОС Linux Ubuntu бесплатное ПО	бесплатно
Microsoft Web Deploy 3.5	бесплатно
MiKTeX 2.9	бесплатно
MSXML 4.0 SP2 Parser and SDK	бесплатно
MySQL Workbench 6.3 CE	бесплатно
NetBeans IDE 8.0.2	бесплатно
Notepad++	бесплатно
Origin 8.1 Sr2	договор №13918/M41 от 24.09.2009 с ЗАО «СофтЛайн Трейд»;
PostgreSQL 9.6	бесплатно
Python 3.4.3	бесплатно
Visual Studio 2010 Prerequisites - English	Акт на передачу прав №785 от 06.08.2021 г.
WCF RIA Services V1.0 SP2	бесплатно
WinDjView 2.1	бесплатно
WinPcap 4.1.3	бесплатно
Wireshark 2.0.0 (64-bit)	бесплатно
R studio	бесплатно

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

Учебная аудитория с мультимедийной установкой (Ноутбук, проектор, колонки), наличие классной доски. Класс ПЭВМ и мультимедийными средствами (проектор, экран, телевизор).

X. Сведения об обновлении рабочей программы дисциплины

№ п.п.	Обновленный раздел рабочей программы дисциплины	Описание внесенных изменений	Дата и протокол заседания кафедры, утвердившего изменения
1.			
2.			