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)

Введение в специальность

Направление подготовки

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»

Для студентов очной формы обучения

СПЕЦИАЛИТЕТ

Для студентов 1 курса

Составитель:
Ю.В. Чемарина

Тверь 2023

I. Аннотация

1. Цель и задачи дисциплины

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

1) системные основы использования математического аппарата будущими специалистами в предметной области;

2) инструментальные средства информационных технологий для защиты информации.

Задачами освоения дисциплины являются:

1) Изучение основных понятий теории защиты информации.

2) Изучение базовых математических методов защиты информации.

3) Получение и систематизация знаний по защищенными компьютерными системам и средствам обработки, хранения и передачи информации; службам защиты информации; математическим моделям процессов, возникающих при защите информации.

4) Изучение механизмов и инструментов кибербезопасности.

5) Изучение карьерных треков в профессиональной сфере, относящейся к информационным технологиям и защите информации.

6) Приобретение навыков самообучения и непрерывного профессионального самосовершенствования.

2. Место дисциплины в структуре ООП

Данная дисциплина входит в обязательную часть учебного плана, является дисциплиной специализации «Математические методы защиты информации» и связана с другими дисциплинами образовательной программы: «Алгебра», «Дискретная математика», «Информатика», «Языки программирования».

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».

Дисциплины, для которых освоение данной дисциплины необходимо как предшествующее: «Основы информационной безопасности», «Аппаратные средства вычислительной техники», «Техническая защита информации», «Теоретико-числовые методы в криптографии», «Методы теории игр в решении задач информационной безопасности», «Методы и средства криптографической защиты информации», «Модели безопасности компьютерных систем», «Защита в операционных системах», «Защита программ и данных», «Защита информации от утечки по техническим каналам», «Теория кодирования, сжатия и восстановления информации», «Проектная деятельность», «Программно-аппаратные средства защиты информации от несанкционированного доступа», «Технология разработки информационных систем в защищенном исполнении», «Основы квантовой физики и информатики», «Теория вычислительной сложности», «Аналитика больших данных», «Проектно-технологическая практика».

3. Объем дисциплины: 6 зачетных единиц, 216 академических часов, в том числе:

контактная аудиторная работа: лекции – 70 часов, в т.ч. практическая подготовка – 0 часов;

самостоятельная работа: 119 часов;

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-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	**ОПК–1.2** 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-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	**ОПК–3.1** Производит стандартные алгебраические операции в основных числовых и конечных полях, кольцах, а также с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ
	ОПК–3.5 Оценивает сложность алгоритмов и вычислений
ОПК–7 Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ	**ОПК–7.2** Применяет известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач
ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства	**ОПК–10.1** Использует методы построения быстрых вычислительных алгоритмов алгебры и теории чисел
	ОПК–10.3 Решает типовые задачи кодирования и декодирования

криптографической защиты информации при решении задач профессиональной деятельности	
ОПК–2.1 Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации	**ОПК–2.1.1** Использует в профессиональной деятельности криптографические алгоритмы и реализует их программно
ОПК-2.3 Способен проводить сравнительный анализ и осуществлять обоснованный выбор программных и программно-аппаратных средств защиты информации с учетом реализованных в них математических методов	**ОПК–2.3.1** Применяет национальные, межгосударственные и международные стандарты в области защиты информации
	ОПК–2.3.2 Анализирует существующие методы и средства, применяемые для контроля и защиты информации

5. Форма промежуточной аттестации и семестр прохождения – зачет в 1-м семестре; экзамен во 2-м 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	
Тема 1. Основные понятия и задачи информационной безопасности	14	4	0	0	10
Тема 2. Основы защиты информации	28	12	0	0	16
Тема 3. Угрозы безопасности защищаемой информации	28	12	0	0	16
Тема 4. Механизмы и инструменты кибербезопасности	17	6	0	0	11

Тема 5. Правовое законодательство в сфере информационной безопасности	9	2	0	0	7
Тема 6. Понятие информации в теории Шеннона	13	4	0	0	9
Тема 7. Кодирование информации	22	6	0	0	16
Тема 8. Основы криптографии	24	6	0	0	18
Тема 9. Технические и программные средства защиты информации	13	4	0	0	9
Тема 10. Компьютерная криминалистика	17	6	0	0	11
Тема 11. Цифровая этика	9	2	0	0	7
Тема 12. Информационная гигиена	9	2	0	0	7
Тема 13. Карьерный навигатор по ИТ-специальностям	13	4	0	0	9
ИТОГО	216	70	0	0	146

III. Образовательные технологии

Учебная программа – наименование разделов и тем	Вид занятия	Образовательные технологии
Тема 1. Основные понятия и задачи информационной безопасности	лекция	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция
Тема 2. Основы защиты информации	лекция	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция
Тема 3. Угрозы безопасности защищаемой информации	лекция	Мозговой штурм, дискуссионные технологии, игровая технология, кейс-технология, методы группового решения творческих задач
Тема 4. Механизмы и инструменты кибербезопасности	лекция	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция

Тема 5. Правовое законодательство в сфере информационной безопасности	лекция	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция
Тема 6. Понятие информации в теории Шеннона	лекция	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция
Тема 7. Кодирование информации	лекция	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция
Тема 8. Основы криптографии	лекция практическая подготовка	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция, игровая технология, кейс-технология, технология развития креативного мышления
Тема 9. Технические и программные средства защиты информации	лекция	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция, кейс-технология, методы группового решения творческих задач
Тема 10. Компьютерная криминалистика	лекция	Мозговой штурм, дискуссионные технологии, игровая технология, кейс-технология, методы группового решения творческих задач
Тема 11. Цифровая этика	лекция	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция
Тема 12. Информационная гигиена	лекция	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция
Тема 13. Карьерный навигатор по ИТ-специальностям	лекция	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция

IV. Оценочные материалы для проведения текущей и промежуточной аттестации

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

<u>Задания для контроля самостоятельной работы</u>

Проверяемые индикаторы достижения компетенций: ОПК-1.2; ОПК-1.3; ОПК-3.1; ОПК-3.5; ОПК-7.2; ОПК-10.1; ОПК-10.3; ОПК-2.1.1; ОПК-2.3.1; ОПК-2.3.2.

Тема 1.

1) Покажите связь между уровнем развития общества и технологиями защиты информации.
2) С чем связан возросший интерес к проблемам защиты информации?
3) В чем, на Ваш взгляд, заключаются основные трудности обеспечения информационной безопасности в настоящее время?
4) Что такое информационная система? Телекоммуникационная система? Автоматизированная система?
5) Что такое защита информации? Информационная безопасность?

Тема 2.

1) Перечислите основные носители информации, особенности их использования и защиты.
2) Какими свойствами определяется ценность информации?
3) Какие критерии оценки ценности информации Вы можете предложить?
4) Приведите примеры различной зависимости ценности информации от времени.
5) Что понимается под информационными ресурсами?

Тема 3.

1) На примере нескольких различных угроз покажите, что их осуществление приведет к изменению одного из основных свойств защищаемой информации (конфиденциальности, целостности, доступности).
2) Приведите примеры систем, для которых наибольшую угрозу безопасности представляет нарушение конфиденциальности информации.
3) Для каких систем (приведите примеры) наибольшую опасность представляет нарушение целостности информации?
4) В каких системах на первом месте стоит обеспечение доступности информации?
5) В чем различие понятий «нарушение конфиденциальности информации», «несанкционированный доступ к информации», «утечка информации»?

Тема 4.

Задание 1.

Примером какой атаки является перехват злоумышленником передаваемых данных с одновременной модификацией «прозрачно» для обеих участвующих в обмене сторон?

A. Прослушивание сети (sniffing)

B. Подмена или спуфинг (spoofing)

C. Перехват соединения (hijacking)

D. Повторная передача (replay)

E. Человек в середине (man in the middle)

Задание 2.

Укажите вид атаки, когда злоумышленник посылает на компьютер специально сконструированный сетевой пакет и получает полный удаленный контроль над этим компьютером.

A. DoS-атака (DoS attack)

B. Переполнение буфера (buffer overflow)

C. Подмена или спуфинг (spoofing)
D. Перехват соединения (hijacking)
E. Повторная передача (replay)

Тема 5.

1) Сформулируйте основные положения Доктрины информационной безопасности РФ.
2) В чем особенности Канадских критериев безопасности компьютерных систем?
3) Опишите структуру Общих критериев безопасности информационных технологий.
4) Опишите технологию применения Общих критериев безопасности информационных технологий.
5) Каковы тенденции развития международной нормативной базы в области информационной безопасности?

Тема 6.

Задание 1.

Какое количество информации связано с исходом следующих опытов:

а) бросок игральной кости;

б) бросок двух монет;

в) вытаскивание наугад одной игральной карты из 36;

г) бросок двух игральных костей.

Задание 2.

Источник порождает множество шестизнаковых сообщений, каждое из которых содержит 1 знак «*», 2 знака «%» и 3 знака «!». Какое количество информации содержится в каждом (одном) из таких сообщений?

Тема 7.

Задание 1.

Первичный алфавит содержит 8 знаков с вероятностями: «пробел» - 0,25; «?» - 0,18; «&» - 0,15; «*» - 0,12; «+» - 0,1; «%» - 0,08; «#» - 0,07 и «!» - 0,05. Предложите вариант неравномерного алфавитного двоичного кода с разделителем знаков, а также постройте коды Шеннона–Фано и Хаффмана; сравните их избыточности.

Задание 2.

Постройте в виде блок-схемы последовательность действий устройства, производящего декодирование сообщения, коды которого удовлетворяют условию Фано. Реализуйте программно на каком-либо языке программирования.

Тема 8.

Задание 1.

Напишите программу работы шифратора-дешифратора по введенному тексту (криптограмме) и ключу для какого-либо алгоритма перестановки.

Задание 2.

Напишите программу работы шифратора-дешифратора по методу гаммирования; битовая гамма должна формироваться программой случайным образом.

Тема 9.

1) Перечислите задачи защиты информации ТКС в условиях конфликта.
2) Дайте определение конфликта. Приведите способы разрешения конфликта в ТКС.
3) Какие виды контроля эффективности инженерно-технической защиты информации вы знаете?
4) Какие предъявляются требования по защите информации от утечки по техническим каналам?
5) Дайте классификацию методов и средств защиты информации от технических разведок.

Тема 10.

Задание 1.

Определите три наиболее важных областей компетенций с точки зрения применимости в компьютерной криминалистике:

- [x] Юридические аспекты права
- [ ] Проектный менеджмент
- [x] Техники расследований
- [x] Компьютерные технологии

Задание 2.

Какой из ниже перечисленных методов относится к специальным методам, применяемым в компьютерной криминалистике:

- (•) Эмуляция сетевых и операционных сервисов
- ( ) Наблюдение
- ( ) Сбор статистических данных
- ( ) Анализ

Тема 11.

Задание 1.

Какие этапы цифровой зрелости проходит государство?

- (•) 1. электронное 2. открытое 3. датацентричное 4. полностью цифровое
- ( ) 1. электронное 2. индустриальное 3. датацентричное 4. цифровое
- ( ) 1. электронное 2. открытое 3. датацентричное 4. полностью цифровое 5. "умное"
- ( ) 1.электронное 2. дистанционное 3. технологичное 4. открытое 5. "умное"

Задание 2.

На каком этапе находится сейчас Россия?

- ( ) электронное государство
- ( ) дистанционное государство
- ( ) цифровое государство
- (•) открытое государство

Тема 12.

Задание 1.

Информационная гигиена - это...?

- способность к поиску, агрегации, проверке достоверности и анализу информации
- совокупность принципов и реальных механизмов, обеспечивающих позитивные взаимодействия этнических и национальных культур, а также сопряженность в общем опыте человечества
- раздел знаний, изучающий закономерности влияния информации на психическое, физическое и социальное здоровье человека и социума в целом
- связь экологических идей с динамикой и свойствами все более плотной, сложной и важной цифровой информационной среды.

Задание 2.

Какое влияние оказывает информационный шум на человека?

- 1. Снижает внимание 2. Повышает утомляемость 3. Провоцирует бессонницу
- 1. Искажение картины мира 2. Формирование выученной беспомощности 3. Развитие клипового мышления 4. Управление впечатлениями
- 1. Эмоциональные расстройства 2. Психологическая зависимость 3. Стресс
- 1. Вызывает любопытство 2. Развивает стрессоустойчивость 3. Повышает умственную работоспособность 4. Стимулирует концентрацию внимания

Тема 13.

Задание 1.

Какие ИТ специальности существуют?

- [x] Back-end разработчик
- [x] UX-дизайнер
- [x] Архитектор
- [ ] IQ-инженер

Задание 2.

Какие типы ИТ компаний вы знаете?

- [x] Веб - сервисы
- [ ] Стартрек
- [x] Разработка игр
- [x] Мобильная разработка

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

Проверяемые индикаторы достижения компетенций: ОПК-1.2; ОПК-1.3; ОПК-3.1; ОПК-3.5; ОПК-7.2; ОПК-10.1; ОПК-10.3; ОПК-2.1.1; ОПК-2.3.1; ОПК-2.3.2.

<u>Вопросы для проведения зачета</u>

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. Определение и классификация НСД. Определение и классификация нарушителя. Классы защищенности АС от НСД к информации.
7. Фундаментальные требования компьютерной безопасности. Требования классов защиты.
8. Удаленные атаки. Классификация удаленных атак.
9. Условия существования вредоносных программ.
10. Причины появления вредоносных программ.
11. Классические компьютерные вирусы. Классификация классических вирусов.
12. Способы заражения компьютерными вирусами.
13. Сетевые черви. Классификация сетевых червей.
14. Троянские программы. Классификация троянских программ.
15. Спам. Основные виды спама.
16. Хакерские утилиты и прочие вредоносные программы.
17. DOS, DDOS –сетевые атаки.

Вопросы для проведения экзамена

1. Структура и состав системы нормативных правовых актов, регулирующих обеспечение информационной безопасности в РФ.
2. Правовой режим защиты государственной тайны.
3. Организация и обеспечение режима секретности.
4. Лицензирование и сертификация в области защиты информации.
5. Правовые основы защиты информации с использованием технических средств.
6. Понятие энтропии.
7. Энтропия и информация.
8. Информация и алфавит.
9. Равномерное алфавитное двоичное кодирование. Байтовый код.
10. Алфавитное неравномерное двоичное кодирование сигналами равной длительности. Коды с разделителем.
11. Префиксные коды.
12. Блочное двоичное кодирование.
13. Код Хемминга.
14. Схема криптосистемы с симметричным шифрованием.
15. Совершенная стойкость шифра. Требования, предъявляемые к ключам.
16. Криптосистемы с открытым ключом.
17. Понятие сертификата. Криптосистема RSA. Выбор параметров.
18. Цифровая подпись. Схемы цифровой подписи.
19. Характеристика инженерно-технической защиты информации как области информационной безопасности.

20. Основные проблемы инженерно-технической защиты информации.
21. Представление сил и средств защиты информации в виде системы.
22. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации.
23. Специальные методы, применяемые в компьютерной криминалистике.
24. Особенности сбора волатильных данных на работающей системе.
25. Основные принципы гуманизма, которые необходимо учитывать при внедрении цифровых технологий.
26. Основные подходы работы с информацией.

V. Учебно-методическое и информационное обеспечение дисциплины

1) Рекомендуемая литература

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.

2) Программное обеспечение

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

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.

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.

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

1. https://cyberleninka.ru/ научная электронная библиотека «Киберленинка»;
2. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru.

VI. Методические материалы для обучающихся по освоению дисциплины

Методические рекомендации по организации самостоятельной работы студентов

Методические рекомендации по организации самостоятельной работы по дисциплине «Введение в специальность» см. в личном кабинете электронной образовательной среды (LMS).

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.

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. Причины, виды, каналы утечки и искажения информации.
22. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.
23. Модели, стратегии и системы обеспечения информационной безопасности.
24. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
25. Общая характеристика методов и средств защиты информации.
26. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности.
27. Программно-аппаратные средства обеспечения информационной безопасности.

Требования к рейтинг-контролю

1-й семестр

Текущая работа обучающихся оценивается в 100 баллов, которые распределяются между двумя модулями (периодами обучения) следующим образом:

Модуль (период обучения)	Максимальная сумма баллов в модуле	Баллы за самостоятельную работу	Баллы за контрольные работы	Баллы за реферат	Баллы за посещаемость и активность
1	40	15	15	-	10
2	60	15	15	20	10

2-й семестр

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

Модуль (период обучения)	Максимальная сумма баллов в модуле	Баллы за самостоятельную работу	Баллы за контрольные работы	Баллы за лабораторную работу	Баллы за посещаемость и активность
1	30	10	15	-	5
2	30	10	5	10	5

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	Комплект учебной мебели, Компьютер:(процессор Core i5-2400+монитор LC E2342T Компьютер:(процессор Core i5-2400+монитор LC E2342T Компьютер:(процессор Core i5-2400+монитор LC E2342T	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

типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, Учебная аудитория. Математический кабинет № 213 (Корпус 3, 170002, Тверская обл., г.Тверь, пер. Садовый, дом 35)	Компьютер:(процессор Core i5-2400+монитор LC E2342T Компьютер:(процессор Core i5-2400+монитор LC E2342T Компьютер:(процессор Core i5-2400+монитор LC E2342T Компьютер:(процессор Core i5-2400+монитор LC E2342T Компьютер:(процессор Core i5-2400+монитор LC E2342T Компьютер:(процессор Core i5-2400+монитор LC E2342T Графопроектор Мультимедийный комплект учебного класса (вариант № 1)Проектор Casio XJ-M140,кронштейн,кабель,удлинитель,настенный проекц. экран Lumien 180*180.ноутбук	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.
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и	Комплект 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 моториз. экраном; Шкаф напольный 19".	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

промежуточной аттестации, Учебная аудитория № 314 (Корпус 3, 170002, Тверская обл., г.Тверь, пер. Садовый, дом 35)		

VIII. Сведения об обновлении рабочей программы дисциплины

№п.п.	Обновленный раздел рабочей программы дисциплины	Описание внесенных изменений	Реквизиты документа, утвердившего изменения
1.	Аннотация	Актуализированы задачи дисциплины, компетенции и их индикаторы. Выделены часы на практическую подготовку	Протокол № 10 от 29.06.2021
2.	Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий	Актуализированы темы занятий	Протокол № 10 от 29.06.2021
3.	Образовательные технологии	Актуализированы темы занятий и соответствующие им образовательные технологии	Протокол № 10 от 29.06.2021
4.	Оценочные материалы для проведения текущей и промежуточной аттестации	Добавлены задания для текущей и промежуточной аттестации	Протокол № 10 от 29.06.2021
5.	Учебно-методическое и информационное обеспечение дисциплины	Обновлен список литературы и перечень ресурсов информационно-телекоммуникационной сети «Интернет»	Протокол № 10 от 29.06.2021
6.	Методические материалы для обучающихся по освоению дисциплины	Актуализированы темы рефератов	Протокол № 10 от 29.06.2021
7.	V. Учебно-методическое и информационное обеспечение дисциплины	Обновление списков ПО. Обновление ссылок из ЭБС.	Протокол № 1 от 1.09.2023