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)

Организационное и правовое обеспечение информационной безопасности

Специальность
10.05.01 Компьютерная безопасность

Специализация
Математические методы защиты информации

Для студентов очной формы обучения

Составитель: к.т.н. П.В. Кратович

Тверь 2023

I. Аннотация

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

Организационное и правовое обеспечение информационной безопасности

2. Цель и задачи дисциплины (или модуля)

Учебная дисциплина «Организационное и правовое обеспечение информационной безопасности» («ОПО ИБ») является важной составляющей общей профессиональной подготовки специалистов в области обеспечения информационной безопасности. Она призвана обеспечить освоение слушателями практических навыков работы с нормативно-правовой базой деятельности в области обеспечения информационной безопасности автоматизированных систем.

3. Место дисциплины (или модуля) в структуре ООП

Дисциплина входит в базовую часть дисциплин. Для усвоения дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплины «Основы информационной безопасности».

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-5 – способностью использовать нормативные правовые акты в своей профессиональной деятельности	**Владеть:** основными методами организационного обеспечения процесса разработки документов и способами обеспечения информационной безопасности **Уметь:** разрабатывать проекты нормативных, организационно-распорядительных и методических документов, регламентирующих функционирование систем защиты информации. **Знать:** нормативные правовые акты в области защиты информации, организационные меры по защите информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.
ПК-14. способностью организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа	**Владеть:** навыками формирования целей, приоритетов, обязанностей и полномочий персонала, обслуживающего средства и системы защиты от НСД. **Уметь:** производить постановку задач персоналу по обеспечению защиты информации и организовывать их выполнение, организовывать перераспределение обязанностей и полномочий персонала. **Знать:** цели и задачи управления персоналом по обеспечению защиты сетей, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.
ПК-15. способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	**Владеть:** навыками планирования мероприятий по обеспечению защиты информации, навыками разработки отчетных документов и разделов технических заданий. **Уметь:** проводить сбор и анализ исходных данных для проектирования и разработки предложений по совершенствованию системы защиты, разрабатывать проекты, планы и графики проведения работ по защите от НСД. **Знать:** нормативные правовые акты в области связи, информатизации и защиты информации, организационные меры по защите информации.
ПК-16. способностью разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие	**Владеть:** навыками разработки нормативных и методических документов. **Уметь:** разрабатывать проекты организационно-распорядительных документов, регламентирующих функционирование системы защиты информации. **Знать:** основные методы организационно обеспечения информационной безопасности.

работу по обеспечению информационной безопасности компьютерных систем	

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

Учебная программа – наименование разделов и тем	Всего (час.)	Контактная работа (час.)		Самостоятельная работа и контроль (час.)
		Лекции	Практические (лабораторные) занятия	
Информационные отношения как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности	12	4		8
Правовой режим защиты государственной тайны	12	4		8
Правовые режимы защиты информации конфиденциального характера	12	4		8
Государственное регулирование деятельности в области защиты информации	6	2		4

Правовая охрана результатов интеллектуальной деятельности	14	5		9
Преступления в сфере компьютерной информации	7	2		5
Понятие организационной защиты информации	7	2		5
Методы обеспечения физической безопасности	12	4		8
Технологические меры поддержания безопасности	8	3		5
Организация режима секретности. Допуск к государственной тайне	9	3		6
Защита компьютерной информации	9	3		6
ИТОГО	108	36		72

Ш. 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)

1. Типовые контрольные задания для проверки уровня сформированности компетенции ОПК-5, ПК-14, ПК-15, ПК-16.

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	1. Раскройте содержание информационной безопасности	Имеется полное верное решение, включающее

владеть	Российской Федерации. 2. Раскройте содержание объектов и субъектов безопасности, объектов и субъектов обеспечения информационной безопасности. 3. Перечислите основные виды обеспечения информационной безопасности и раскройте их содержание. 4. Перечислите наиболее важные объекты информационной безопасности организации и угрозы безопасности этих объектов.	правильный ответ – 3 балла Решение не дано или дано неверное решение – 0 баллов
базовый уметь	1. Составьте перечень контрольных мероприятий и действий по оценке уровня безопасности объекта. 2. Опишите организацию конфиденциального делопроизводства 3. Опишите структуру системы обеспечения информационной безопасности организации.	Имеется полное верное решение, включающее правильный ответ – 3 балла Решение не дано или дано неверное решение – 0 баллов
базовый знать	1. Каковы основные формы и свойства информации? 2. Какие существуют особенности документального оформления политики безопасности, и чем они объясняются? 3. Как организуются допуск и доступ к сведениям, составляющим государственную тайну?	Имеется полное верное решение, включающее правильный ответ – 3 балла Решение не дано или дано неверное решение – 0 баллов

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

а) Основная литература:

1. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ В.Ф. Шаньгин.— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 702 с.— Режим доступа: http://www.iprbookshop.ru/63594.html. — ЭБС «IPRbooks»

2. Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ С.В. Петров, П.А Кисляков.— Электрон. текстовые

данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 с.— Режим доступа: http://www.iprbookshop.ru/33857.html. — ЭБС «IPRbooks»

б) Дополнительная литература

1. Чепурнова Н.М. Правовые основы информатики [Электронный ресурс]: учебное пособие для студентов вузов, обучающихся по направлению «Прикладная информатика»/ Н.М. Чепурнова, Л.Л Ефимова.— Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2015.— 295 с.— Режим доступа: http://www.iprbookshop.ru/34498.html. — ЭБС «IPRbooks»

2. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ А.В. Артемов.— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 с.— Режим доступа: http://www.iprbookshop.ru/33430.html. — ЭБС «IPRbooks»

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.
1. 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 I. Правовое обеспечение информационной безопасности

Тема 1.1 Информационные отношения как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности

Структура информационной сферы и характеристика ее элементов. Информация как объект правоотношений. Категории информации по условиям доступа к ней и распространения. Конституционные гарантии прав граждан в информационной сфере и механизм их реализации.

Понятие информационной безопасности. Субъекты и объекты правоотношений в области информационной безопасности. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в Российской Федерации Понятие и виды защищаемой информации по законодательству РФ. Перспективы развития законодательства в области информационной безопасности.

Тема 1.2. Правовой режим защиты государственной тайны

Понятие правового режима защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Принципы и механизмы отнесения сведений к государственной тайне, их

засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Система контроля за состоянием защиты государственной тайны. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная).

Тема 1.3. Правовые режимы защиты информации конфиденциального характера

Понятие информации конфиденциального характера по российскому законодательству. Основные виды «конфиденциальной» информации: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, профессиональная тайна, тайна следствия и судопроизводства.

Правовые режимы «конфиденциальной» информации: содержание и особенности. Основные требования, предъявляемые к организации защиты конфиденциальной информации.

Юридическая ответственность за нарушения правовых режимов «конфиденциальной» информации (дисциплинарная, гражданско-правовая, административная и уголовная).

Тема 1.4. Государственное регулирование деятельности в области защиты информации

Понятие лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию. Правовая регламентация лицензионной деятельности в области обеспечения информационной безопасности. Объекты лицензирования и участники лицензионных отношений в сфере защиты информации. Органы лицензирования и их полномочия. Организация лицензирования в сфере обеспечения информационной безопасности. Контроль за соблюдением лицензиатами условий ведения деятельности.

Понятие подтверждения соответствия по российскому законодательству, формы подтверждения. Правовая регламентация сертификационной

деятельности в области обеспечения информационной безопасности. Режимы сертификации. Объекты сертификационной деятельности (сертификации). Органы сертификации и их полномочия.

Тема 1.5. Правовая охрана результатов интеллектуальной деятельности

Законодательство РФ об интеллектуальных правах. Понятие и виды интеллектуальных прав. Объекты и субъекты авторского права. Авторские права (личные неимущественные права и исключительное право). Правовая охрана баз данных, топологий интегральных микросхем и единых технологий.

Защита интеллектуальных прав. Юридическая ответственность за нарушение авторских прав.

Тема 1.6. Преступления в сфере компьютерной информации

Преступления в сфере компьютерной информации: виды, состав. Основы расследования преступлений в сфере компьютерной информации. Иные преступления в информационной сфере.

Раздел II. Организационное обеспечение информационной безопасности

Тема 2.1. Понятие организационной защиты информации

Сущность организационных методов защиты информации. Соотношение организационных методов защиты информации с правовыми и техническими.

Понятие «режим защиты информации». Режим защиты информации как составная часть организационной защиты информации.

Тема 2.2. Методы обеспечения физической безопасности

Объекты обеспечения физической безопасности: сооружения, предметы, люди. Проектирование здания. Охрана территории. Охрана здания. Сигнализация. Противостояние взлому: двери, замки, запоры,

ограждения. Безопасность при транспортировке носителей информации. Личная безопасность сотрудников и членов их семей. Защита документов от подделок. Обнаружение фальсификации документов. Предварительная защита документов. Приборы и методы контроля документов. Хранилища. Сейфы. Запирающие устройства. Физическая защита неподвижных объектов. Пропускной режим.

Тема 2.3. Технологические меры поддержания безопасности

Проблема безопасности технологии. Организация работы персонала. Резервирование оборудования и дублирование информации. Система инструкций и правил. Администрирование технологического процесса. Контроль доступа и средства поиска и досмотра. Системы контроля доступа. Технология считывания ключей. Средства поиска и досмотра. Обнаружение металлов и взрывчатки. Обнаружители наркотиков. Обнаружители газов и отравляющих веществ. Обнаружители радиоактивных веществ.

Тема 2.4. Организация режима секретности

Организационные меры, направленные на защиту государственной тайны. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны. Виды представления информации. Пути прохождения информации. Учет получения, перемещения, преобразования, хранения и уничтожения информации. Секретариаты. Первые отделы. Служба собственной безопасности. Категорирование объектов. Подбор и расстановка кадров.

Тема 2.5. Допуск к государственной тайне

Порядок допуска и доступа к государственной тайне. Основные принципы допускной работы. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения. Документальное оформление для отправки на согласование.

Процедура оформления и переоформления допусков и ее документирование, подлежащие согласованию с органами государственной безопасности. Особенности инструктажа и документальное оформление контракта об оформлении допуска к государственной тайне.

Тема 2.6. Защита компьютерной информации

Технологическая схема обработки информации. Основные каналы утечки информации при обработке на компьютерах. Аппаратные закладки. Виброаккустический канал утечки информации. Визуальный канал утечки информации. Программные и аппаратные средства защиты от несанкционированного доступа. Парольная система доступа. Защита на различных уровнях: операционная система, прикладные программы. Программные закладки. Разграничение доступа. Регистрация. Остаточная информация. Защита от копирования.

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. Структура информационной сферы и характеристика ее элементов.
2. Категории информации по условиям доступа к ней и распространения.
3. Конституционные гарантии прав граждан в информационной сфере и механизм их реализации.
4. Понятие информационной безопасности.
5. Субъекты и объекты правоотношений в области информационной безопасности.
6. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в Российской Федерации.
7. Понятие и виды защищаемой информации по законодательству РФ.
8. Понятие правового режима защиты государственной тайны.
9. Государственная тайна как особый вид защищаемой информации и ее характерные признаки.
10. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации.
11. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания.
12. Органы защиты государственной тайны и их компетенция. Система контроля за состоянием защиты государственной тайны. Юридическая ответственность за нарушения правового режима защиты государственной тайны.
13. Понятие информации конфиденциального характера по российскому законодательству.
14. Основные виды «конфиденциальной» информации.
15. Основные требования, предъявляемые к организации защиты конфиденциальной информации.
16. Юридическая ответственность за нарушения правовых режимов «конфиденциальной» информации.
17. Понятие лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию.

18. Правовая регламентация лицензионной деятельности в области обеспечения информационной безопасности.
19. Объекты лицензирования и участники лицензионных отношений в сфере защиты информации.
20. Организация лицензирования в сфере обеспечения информационной безопасности. Контроль за соблюдением лицензиатами условий ведения деятельности.
21. Правовая регламентация сертификационной деятельности в области обеспечения информационной безопасности.
22. Режимы сертификации. Объекты сертификации. Органы сертификации и их полномочия.
23. Законодательство РФ об интеллектуальных правах. Понятие и виды интеллектуальных прав.
24. Объекты и субъекты авторского права. Правовая охрана баз данных, топологий интегральных микросхем и единых технологий.
25. Защита интеллектуальных прав. Юридическая ответственность за нарушение авторских прав.
26. Преступления в сфере компьютерной информации: виды, состав.
27. Основы расследования преступлений в сфере компьютерной информации.
28. Сущность организационных методов защиты информации. Соотношение организационных методов защиты информации с правовыми и техническими.
29. Понятие «режим защиты информации». Режим защиты информации как составная часть организационной защиты информации.
30. Проблема безопасности технологии. Организация работы персонала.
31. Резервирование оборудования и дублирование информации. Система инструкций и правил.
32. Администрирование технологического процесса. Контроль доступа и средства поиска и досмотра. Системы контроля доступа. Технология считывания ключей.

33. Организационные меры, направленные на защиту государственной тайны. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны.
34. Виды представления информации. Пути прохождения информации. Учет получения, перемещения, преобразования, хранения и уничтожения информации.
35. Порядок допуска и доступа к государственной тайне. Основные принципы допускной работы.
36. Процедура оформления и переоформления допусков и ее документирование, подлежащие согласованию с органами государственной безопасности.
37. Особенности инструктажа и документальное оформление контракта об оформлении допуска к государственной тайне.
38. Технологическая схема обработки информации. Основные каналы утечки информации при обработке на компьютерах.
39. Программные и аппаратные средства защиты от несанкционированного доступа.
40. Разграничение доступа.

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

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 № 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

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 № 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
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, Компьютерный класс математического факультета № 16 (Корпус 3, 170002, Тверская обл., г.Тверь, пер. Садовый, дом 35)	Набор учебной мебели, меловая доска, Компьютер INT Allegro, монитор Benq 24" GL2460 – 10 шт.

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

№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 01.09.2017
7.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Дополнение списков. Обновление ссылок из ЭБС.	Протокол № 1 от 01.09.2023