Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Директор
_____ А. В. Замятин
«16» мая 2022 г.

Рабочая программа дисциплины

Организационное и правовое обеспечение информационной безопасности

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки :
Интеллектуальный анализ больших данных

Форма обучения
Очная

Квалификация
Магистр

Год приема
2022

Код дисциплины в учебном плане: Б1.В.ДВ.03.02.02

СОГЛАСОВАНО:
Руководитель ОП
_____А.В. Замятин

Председатель УМК
_____С.П. Сущенко

Томск – 2022

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

– ОПК-4 – способность комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности;

– ПК-1 – способность разрабатывать и применять математические методы, алгоритмы, программное обеспечение для решения задач научно-исследовательской и проектной деятельности.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИПК-1.2 Применяет существующие математические методы, алгоритмы и программное обеспечение для решения задач в области профессиональной деятельности.

ИОПК-4.2 Учитывает основные требования информационной безопасности.

2. Задачи освоения дисциплины

– Ознакомить студентов с основными законодательными и подзаконными актами в области защиты информации;

– Научить использовать нормативные правовые акты и методические документы в области информационной безопасности, в т.ч. регулирующие вопросы организации лицензирования и оценки соответствия в Российской Федерации; обучить анализу и оценке угроз информационной безопасности, в частности, связанных с утечкой информации по техническим каналам утечки информации, а также выявляемых при разработке системы защиты информации в информационных системах персональных данных;

– Обучить общим принципам организации защиты информации с применением модели угроз и модели нарушителя.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений, предлагается обучающимся на выбор. Дисциплина входит в минор по выбору «Введение в информационную безопасность».

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Третий семестр, зачет

5. Входные требования для освоения дисциплины

Для освоения дисциплины необходимо знать общие методы обеспечения информационной безопасности и основные типы средств обеспечения информационной безопасности.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 3 з.е., 108 часов, из которых:
-лекции: 32 ч.
в том числе практическая подготовка: 0 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Раздел 1. Введение

1.1. Введение в правовые основы. Информация как объект права.

1.2. Правовое регулирование в области защиты информации. Органы исполнительной власти, осуществляющие регулирование.

1.3. Закон об информации, информационных технологиях и защите информации. Регулирование использования международной сети Интернет.

Раздел 2. Лицензирование и оценка соответствия

2.1. Лицензирование в области защиты информации.

2.2. Формы оценки соответствия. Сертификация средств защиты информации по требованиям безопасности.

2.3. Аккредитация.

2.4. Аттестация объектов информатизации. Нормативные документы ФСБ и ФСТЭК по аттестации.

Раздел 3. Технические каналы утечки информации

3.1. Технические каналы утечки информации.

Раздел 4. Законодательство в области защиты персональных данных

4.1. Общие сведения по законодательству в области персональных данных.

4.2. Закон о персональных данных. Уровни защищенности информационных систем персональных данных.

4.3. Требования ФСБ по защите информационных систем персональных данных.

4.4. Требования ФСТЭК по защите информационных систем персональных данных.

4.5. Модели угроз. Оценка актуальности угроз.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля выполнения домашних заданий по темам лекций и проведения коллоквиума по первому и второму разделам дисциплины в середине семестра.

Домашние задания:

Задание 1.

Найти и выбрать сертифицированное средство защиты информации (СЗИ), соответствующее заданным параметрам. Описать характеристики выбранного СЗИ, соответствующие определенным нормативными документами ФСБ и ФСТЭК России требованиям.

Задание 2.

Описать возможные технические каналы утечки информации для заданного объекта информатизации и способы их нейтрализации.

Задание 3.

Определить уровень защищенности и актуальные угрозы информационной безопасности для заданной информационной системы персональных данных. Определить перечень мер и средств защиты информации, необходимых для нейтрализации выявленных угроз.

Темы опросов на занятиях:

1. Система обеспечения информационной безопасности Российской Федерации. Регулирование процесса обеспечения информационной безопасности Российской Федерации.
2. Лицензирование в области информационной безопасности. Сертификация средств защиты информации.
3. Аккредитация. Аттестация объектов информатизации.
4. Принципы реализации технических каналов утечки информации.
5. Этапы построения системы защиты информации в организации.

6. Этапы определения уровня защищенности информационных систем персональных данных и актуальных угроз безопасности персональных данных.

Вопросы для коллоквиума:

1. Организационные и правовые меры по защите информации. Государственные органы Российской Федерации в области защиты информации.
2. Основные нормативно-правовые акты в области информационной безопасности.
3. Виды конфиденциальной информации.
4. Лицензирование в области информационной безопасности.
5. Сертификация в области информационной безопасности, нормативно-правовые акты, руководящие документы.
6. Аккредитация в области защиты информации.
7. Аттестация объектов информатизации.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Промежуточная аттестация осуществляется в письменном виде при условии успешной сдачи коллоквиума.

Типовые задания для проведения промежуточной аттестации по дисциплине:

1. Организационные и правовые меры по защите информации. Государственные органы РФ в области защиты информации.
2. Основные нормативно-правовые акты в области информационной безопасности.
3. Виды конфиденциальной информации.
4. Лицензирование в области информационной безопасности, нормативно-правовые акты.
5. Сертификация в области информационной безопасности, нормативно-правовые акты, руководящие документы.
6. Аккредитация в области защиты информации.
7. Аттестация объектов информатизации.
8. Технические каналы утечки акустической информации.
9. Технические каналы утечки информации, обрабатываемой с использованием основных технических средств и систем.
10. Этапы построения системы защиты информации в организации.
11. Модель угроз информационной безопасности. Основные положения.
12. Модель нарушителя информационной безопасности. Основные положения.
13. Законодательство в области защиты персональных данных. Этапы определения уровня защищенности информационных систем персональных данных.
14. Модель угроз информационной системы персональных данных. Оценка актуальности угроз.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle»

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине.

12. Перечень учебной литературы и ресурсов сети Интернет

№ п/п	Авторы / составители	Заглавие	Издательство	Год издания, количество страниц

Основная литература				
1.	Федеральное собрание Российской Федерации	Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»	-	2006 г.
2.	Федеральное собрание Российской Федерации	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»	-	2006 г.
3.	Президент Российской Федерации	Указ президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»	-	2016 г.
4.	Федеральное государственное учреждение «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (утвержден Федеральным агентством по техническому регулированию и метрологии)	ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» от 27.12.2006 г.	-	2006 г.
5.	Федеральное государственное учреждение «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю»; Общество с ограниченной ответственностью «Научно-производственная фирма «Кристалл» (утвержден Федеральным агентством по	ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» от 18.12.2008 г.	-	2008 г.

	техническому регулированию и метрологии)			
6.	Бирюков А.А.	Информационная безопасность: защита и нападение	М.: ДМК Пресс	2016 г., 474 с.
7.	Аверченков В.И., Рытов М.Ю., Гайнулин Т.Р.	Защита персональных данных в организации	М.: ФЛИНТА	2016 г, 124 с.
8.	Каторин Ю.Ф., Разумовский А.В., Спивак А.И.	Защита информации техническими средствами	СПб: НИУ ИТМО	2012 г., 416 с.
9.	Чубукова С.Г.	Организационное и правовое обеспечение информационной безопасности. Учебник и практикум	М.: Юрайт	2016 г., 326 с.
10.	Правительство Российской Федерации	Постановление Правительства Российской Федерации от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»	-	2012 г.
11.	Правительство Российской Федерации	Постановление Правительства Российской Федерации от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд	-	2012 г.

		юридического лица или индивидуального предпринимателя)»		
12.	Правительство Российской Федерации	Постановление Правительства РФ от 26.06.1995 № 608 «О сертификации средств защиты информации»	-	1995 г.
13.	Федеральная служба по техническому и экспортному контролю Российской Федерации	Приказ ФСТЭК России от 10.04.2015 № 33 «Об утверждении Правил выполнения отдельных работ по аккредитации органов по сертификации и испытательных лабораторий, выполняющих работы по оценке (подтверждению) соответствия в отношении продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, в установленной ФСТЭК России сфере деятельности»	-	2015 г.
14.	Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации	Приказ Минцифры России от 29 октября 2020 года № 559 «Об утверждении Административного регламента предоставления Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации государственной услуги по аккредитации удостоверяющих центров и Административного регламента осуществления Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации государственного контроля (надзора) за соблюдением аккредитованными удостоверяющими центрами требований, которые установлены Федеральным законом "Об электронной подписи" и на соответствие которым эти удостоверяющие	-	2020 г.

		центры были аккредитованы»		
15.	Государственная техническая комиссия при Президенте Российской Федерации	Положение по аттестации объектов информатизации по требованиям безопасности информации (утверждено Гостехкомиссией РФ 25.11.1994)	-	1994 г.
16.	Федеральная служба по техническому и экспортному контролю Российской Федерации	Приказ ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»	-	2021 г.
17.	Правительство Российской Федерации	Постановление Правительства РФ от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"	-	2012 г.
18.	Федеральная служба по техническому и экспортному контролю Российской Федерации	Приказ ФСТЭК России от 18 февраля 2013 года № 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"	-	2013 г.
19.	Федеральная служба безопасности Российской Федерации	Приказ ФСБ РФ от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»	-	2014 г.
Дополнительная литература				
20.	Мельников В.П., Куприянов А.И.	Информационная безопасность	М.: КНОРУС	2018 г., 268 с.
21.	Ковалева Н.Н.	Информационное право в	М.: Дашков и КО	2007 г., 360 с.

		России. Учебное пособие		
22.	Жарова А.К.	Право и информационные конфликты в информационно-телекоммуникационной сфере	М.: Янус	2016 г., 248 с.
23.	Бузов Г.А., Калинин С.В., Кондратьев А.В.	Защита от утечки по техническим каналам: Учебное пособие	М.: Горячая линия-Телеком	2005 г., 416 с.
24.	Федеральное государственное учреждение «32 Государственный научно-исследовательский испытательный институт Минобороны России»; Федеральное государственное учреждение «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (утвержден Федеральным агентством по техническому регулированию и метрологии)	ГОСТ Р 53112-2008 «Защита информации. Комплексы для измерений параметров побочных электромагнитных излучений и наводок. Технические требования и методы испытаний» от 18.12.2008 г.	-	2008 г.

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:
– MS Windows; MS Office.

б) информационные справочные системы:
– http://www.kremlin.ru/acts/bank
– http://pravo.gov.ru
– http://www.consultant.ru
– https://docs.cntd.ru
– https://base.garant.ru

14. Материально-техническое обеспечение

Для реализации дисциплины необходимы лекционные аудитории и аудитории для проведения практических занятий. Специальные технические средства (проектор, компьютер и т.д.) требуются для демонстрации материала в рамках изучаемых разделов.

15. Информация о разработчиках

Генрих Виктор Витальевич, ассистент кафедры компьютерной безопасности ТГУ.