

МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ

Директор института прикладной
математики и компьютерных наук

А.В. Замятин

2021 г.



**Организационное и правовое обеспечение
информационной безопасности**

рабочая программа дисциплины

Закреплена за кафедрой	<i>компьютерной безопасности</i>
Учебный план	<i>10.05.01 Компьютерная безопасность, профиль «Анализ безопасности компьютерных систем»</i>
Форма обучения	<i>очная</i>
Общая трудоёмкость	<i>3 з.е.</i>
Часов по учебному плану	<i>108</i>
в том числе:	
аудиторная контактная работа	<i>33,85</i>
самостоятельная работа	<i>74,15</i>
Вид(ы) контроля в семестрах	
экзамен/зачет/зачет с оценкой	<i>Семестр В – зачет</i>

Программу составил:
ассистент кафедры компьютерной безопасности



В.В. Генрих

Рецензент:
канд. техн. наук, доцент,
заведующий кафедрой компьютерной безопасности



С.А. Останин

Рабочая программа дисциплины «Организационное и правовое обеспечение информационной безопасности» разработана в соответствии с образовательным стандартом высшего образования – специалитет, самостоятельно устанавливаемым федеральным государственным автономным образовательным учреждением высшего образования «Национальный исследовательский Томский государственный университет» по специальности 10.05.01 Компьютерная безопасность (Утвержден Ученым советом НИ ТГУ, протокол от 30.06.2021 г. № 06).

Рабочая программа одобрена на заседании кафедры компьютерной безопасности

Протокол от 02 июня 2021 г. № 06

Заведующий кафедрой компьютерной безопасности,
канд. техн. наук, доцент



С.А. Останин

Рабочая программа одобрена на заседании учебно-методической комиссии института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от 17 июня 2021 г. № 05

Председатель УМК ИПМКН,
д-р техн. наук, профессор



С.П. Сущенко

Цель освоения дисциплины

Цель – 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.

1. Место дисциплины в структуре ОПОП

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к обязательной части Блока 1 «Дисциплины», входит в модуль «Общие вопросы компьютерной безопасности».

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

Пререквизиты дисциплины: нет.

Постреквизиты дисциплины: учебная и производственная практика, Научно-исследовательская работа.

2. Компетенции и результаты обучения, формируемые в результате освоения дисциплины

Таблица 1.

Компетенция	Индикатор компетенции	Код и наименование результатов обучения (планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций)
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ИОПК-5.1 Обладает необходимыми знаниями нормативно-правовой базы, регламентирующей деятельность по защите информации; ИОПК-5.2 Определяет подлежащие применению нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.	ОР-5.1.1 Обучающийся сможет: - использовать нормативные правовые акты в области защиты информации (в т.ч. при реализации/модернизации системы защиты информации объекта информатизации). ОР-5.1.2 Обучающийся сможет: - анализировать основные правовые акты, давать правовую оценку информации, используемой в профессиональной деятельности. ОР-5.2.1 Обучающийся сможет: - подбирать и изучать научно-техническую литературу, изучать и отбирать правовые и нормативные акты в области обеспечения информационной безопасности.
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными	ИОПК-6.1 Понимает нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; ИОПК-6.2 Предпринимает	ОР-6.1.1 Обучающийся сможет: - понимать и использовать применяемые в сфере защиты информации нормативные правовые акты и методические документы (в т.ч. Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю).

<p>правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю</p>	<p>необходимые действия по организации защиты информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.</p>	<p>ОР-6.2.1 Обучающийся сможет: - анализировать и оценивать угрозы информационной безопасности объекта защиты информации.</p> <p>ОР-6.2.2 Обучающийся сможет: - применять нормативные правовые акты и нормативные методические документы в области защиты информации (в т.ч. Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю), определяющие вопросы внедрения/применения средств и мер по защите информации, в т.ч. в компьютерных системах, а также разрабатывать проекты нормативных документов, регламентирующих обеспечение информационной безопасности в организации.</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3. Структура и содержание дисциплины

3.1. Структура и трудоемкость видов учебной работы по дисциплине

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

Таблица 2.

Вид учебной работы	Трудоемкость в академических часах	
Общая трудоемкость	108	108
Контактная работа:	33,85	33,85
Лекции (Л):	32	32
Практики (ПЗ)		
Лабораторные работы (ЛР)		
Семинары (СЗ)		
Групповые консультации	1.6	1.6
Индивидуальные консультации		
Промежуточная аттестация	0.25	0.25
Самостоятельная работа обучающегося:	74,15	74,15
<i>- выполнение домашних заданий</i>	24	24
<i>- изучение учебного материала</i>	30	30
<i>- подготовка к промежуточной аттестации по форме зачета</i>	20,15	20,15
Вид промежуточной аттестации (зачет, зачет с оценкой, экзамен)	Зачет	Зачет

3.2. Содержание и трудоемкость разделов дисциплины

Таблица 3.

Код занятия	Наименование разделов и тем и их содержание	Вид учебной работы, занятий, контроля	С е м е с т р	Часы в электронной форме	Всего (час.)	Литература	Код (ы) результата(ов) обучения
	Раздел 1. Введение		3		11	1, 3, 4, 5, 6, 9, 22, 23, 24	ОР-5.1.1, ОР-5.1.2, ОР-5.2.1
1.1.	Введение в правовые основы. Информация как объект права.	Лекции	3		1		
1.2	Правовое регулирование в области защиты информации. Органы исполнительной власти, осуществляющие регулирование.	Лекции	3		3		
1.3	Закон об информации, информационных технологиях и защите информации. Регулирование использования международной сети Интернет.	Лекции	3		3		
1.4	Изучение учебного материала.	СРС	3		4		
	Раздел 2. Лицензирование и оценка соответствия		3		29	4, 5, 10, 11, 12, 13, 14, 15, 16, 17	ОР-5.1.1, ОР-5.1.2, ОР-6.1.1, ОР-6.2.1, ОР-6.2.2
2.1.	Лицензирование в области защиты информации.	Лекции	3		3		
2.2.	Формы оценки соответствия. Сертификация средств защиты информации по требованиям безопасности.	Лекции	3		3		
2.3	Аккредитация.	Лекции	3		1		
2.4	Аттестация объектов информатизации. Нормативные документы по аттестации.	Лекции	3		2		
2.5	Изучение учебного материала.	СРС	3		11		
	Выполнение домашних заданий.	СРС	3		8		
	Текущий контроль успеваемости (коллоквиум)	Лекции	3		1		
	Раздел 3. Технические каналы утечки информации		3		11	4, 8, 25, 26	ОР-5.1.1, ОР-5.2.1, ОР-6.2.1, ОР-6.2.2
3.1.	Технические каналы утечки информации.	Лекции	3		3		
3.2	Изучение учебного материала.	СРС	3		3		
	Выполнение домашних заданий.	СРС	3		5		
	Раздел 4. Законодательство в области защиты персональных данных		3		35	2, 7, 9, 18, 19, 20, 21	ОР-5.1.1, ОР-5.1.2, ОР-5.2.1, ОР-6.2.1, ОР-6.2.2
4.1.	Общие сведения по законодательству в области персональных данных.	Лекции	3		1		
4.2.	Закон о персональных данных. Уровни защищенности информационных систем персональных данных.	Лекции	3		2		

4.3.	Требования ФСБ по защите информационных систем персональных данных.	Лекции	3		2		
4.4.	Требования ФСТЭК по защите информационных систем персональных данных.	Лекции	3		4		
4.5.	Модели угроз. Оценка актуальности угроз.	Лекции	3		3		
4.6	Изучение учебного материала.	СРС	3		12		
	Выполнение домашних заданий.	СРС	3		11		
	Консультации в период теоретического обучения		3		1,6		
	Подготовка к промежуточной аттестации в форме зачета	СРС	3		20,15	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26	
	Прохождение промежуточной аттестации в форме зачета	За	3		0,25		

4. Образовательные технологии, учебно-методическое и информационное обеспечение для освоения дисциплины

Занятия по дисциплине проводятся в классической форме в виде лекций:

- лекции – в виде классического изложения преподавателем основного теоретического материала. В начале лекции проводится быстрый устный опрос по пройденному материалу, который необходим для проведения текущей лекции. В конце лекции подводится краткий итог (перечисление) основных положений, пройденных на лекции. По итогу прохождения основных тематических блоков дисциплины предусмотрено проведение опросов в письменном виде.

Обязательными при изучении дисциплины «Организационное и правовое обеспечение информационной безопасности» являются следующие виды самостоятельной работы:

- разбор теоретического материала по конспектам лекций, учебным пособиям и научным статьям;
- выполнение домашних заданий по темам лекций.

Для текущего контроля самостоятельной работы студентов в середине семестра предусмотрено проведение коллоквиума по первому и второму разделам дисциплины.

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

Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения, характеризующих этапы формирования компетенций, и методические материалы, определяющие процедуры оценивания результатов обучения, приведены в Приложении 1 к рабочей программе «Фонд оценочных средств».

Типовые контрольные задания или иные материалы, необходимые для текущей аттестации, и методические материалы, определяющие процедуры оценивания результатов текущей аттестации, приведены в Приложении 2 к рабочей программе «Примерные оценочные средства текущей аттестации».

4.1. Рекомендуемая литература и учебно-методическое обеспечение

№ 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»	ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» от 27.12.2006 г.	-	2006 г.

	(утвержден Федеральным агентством по техническому регулированию и метрологии)			
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 техническому регулированию и метрологии)	ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» от 18.12.2008 г.	-	2008 г.
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	-	2012 г.

		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 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.	Федеральная служба безопасности Российской Федерации	Приказ ФСБ РФ от 29.12.2020 № 639 «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации»	-	2020 г.
15.	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 центры были аккредитованы»	-	2020 г.

16.	Государственная техническая комиссия при Президенте Российской Федерации	Положение по аттестации объектов информатизации по требованиям безопасности информации (утверждено Гостехкомиссией РФ 25.11.1994)	-	1994 г.
17.	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.
18.	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.
19.	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.
20.	Федеральная служба безопасности Российской Федерации	Приказ ФСБ РФ от 10 июля 2014 г. № 378 «Об утверждении Состав 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.
21.	Федеральная служба безопасности Российской Федерации	Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности (утверждены руководством 8 Центра ФСБ России от 31 марта 2015 года N 149/7/2/6-432)	-	2015 г.
Дополнительная литература				
22.	Мельников В.П., Куприянов А.И.	Информационная безопасность	М.: КНОРУС	2018 г., 268 с.
23.	Ковалева Н.Н.	Информационное право в России. Учебное пособие	М.: Дашков и КО	2007 г., 360 с.
24.	Жарова А.К.	Право и информационные конфликты в информационно-телекоммуникационной сфере	М.: Янус	2016 г., 248 с.
25.	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.
26.	Федеральное государственное	ГОСТ Р 53112-2008 «Защита информации. Комплексы для измерений	-	2008 г.

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)	параметров побочных электромагнитных излучений и наводок. Технические требования и методы испытаний» от 18.12.2008 г.		
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------	--	--

4.2. Базы данных и информационно-справочные системы, в том числе зарубежные

1. Электронный ресурс:
<http://www.kremlin.ru/acts/bank>
2. Электронный ресурс:
<http://pravo.gov.ru>
3. Электронный ресурс:
<http://www.consultant.ru>
4. Электронный ресурс:
<https://docs.cntd.ru>
5. Электронный ресурс:
<https://base.garant.ru>

4.3. Перечень лицензионного и программного обеспечения

MS Windows; MS Office.

4.4. Оборудование и технические средства обучения

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.

5. Методические указания обучающимся по освоению дисциплины

Основой обучения является курс лекций, читаемый преподавателем. Для самостоятельной работы и дополнительного расширения круга знаний рекомендуется использовать литературу, приведенную в разделе 4.1, а также информационные системы, приведенные в разделе 4.2.

6. Преподавательский состав, реализующий дисциплину

Генрих Виктор Витальевич, ассистент кафедры компьютерной безопасности ТГУ.

7. Язык преподавания – русский язык.