АНТИПЛАГИАТ
ОБНАРУЖЕНИЕ ЗАИМСТВОВАНИЙ

Отчет предоставлен сервисом «Антиплагиат» - http://tusur.antiplagiat.ru

Отчет о проверке

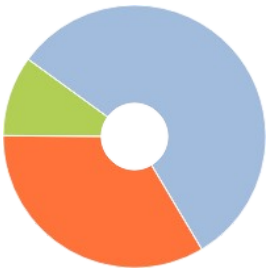
Автор: Основная Почта Лоцман

Название документа: КП Информационное право.docx

Проверяющий: Основная Почта Лоцман

Организация: ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ"

РЕЗУЛЬТАТЫ ПРОВЕРКИ



Совпадения: 33,51%

Оригинальность: 56,65%

Цитирования: 9,84%

Самоцитирования: 0%

«Совпадения», «Цитирования», «Самоцитирования», «Оригинальность» являются отдельными показателями, отображаются в процентах и в сумме дают 100%, что соответствует проверенному тексту документа.

Проверено: 93,76% текста документа, исключено из проверки: 6,24% текста документа. Разделы, отключенные пользователем: Титульный лист, Библиография

- **Совпадения** — фрагменты проверяемого текста, полностью или частично сходные с найденными источниками, за исключением фрагментов, которые система отнесла к цитированию или самоцитированию. Показатель «Совпадения» – это доля фрагментов проверяемого текста, отнесенных к совпадениям, в общем объеме текста.
- **Самоцитирования** — фрагменты проверяемого текста, совпадающие или почти совпадающие с фрагментом текста источника, автором или соавтором которого является автор проверяемого документа. Показатель «Самоцитирования» – это доля фрагментов текста, отнесенных к самоцитированию, в общем объеме текста.
- **Цитирования** — фрагменты проверяемого текста, которые не являются авторскими, но которые система отнесла к корректно оформленным. К цитированиям относятся также шаблонные фразы; библиография; фрагменты текста, найденные модулем поиска «СПС Гарант: нормативно-правовая документация». Показатель «Цитирования» – это доля фрагментов проверяемого текста, отнесенных к цитированию, в общем объеме текста.
- **Текстовое пересечение** — фрагмент текста проверяемого документа, совпадающий или почти совпадающий с фрагментом текста источника.
- **Источник** — документ, проиндексированный в системе и содержащийся в модуле поиска, по которому проводится проверка.
- **Оригинальный текст** — фрагменты проверяемого текста, не обнаруженные ни в одном источнике и не отмеченные ни одним из модулей поиска. Показатель «Оригинальность» – это доля фрагментов проверяемого текста, отнесенных к оригинальному тексту, в общем объеме текста.

Обращаем Ваше внимание, что система находит текстовые совпадения проверяемого документа с проиндексированными в системе источниками. При этом система является вспомогательным инструментом, определение корректности и правомерности совпадений или цитирований, а также авторства текстовых фрагментов проверяемого документа остается в компетенции проверяющего.

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

Номер документа: 37138

Тип документа: Не указано

Дата проверки: 05.07.2025 17:02:09

Дата корректировки: Нет

Количество страниц: 34

Символов в тексте: 56053

Слов в тексте: 6043

Число предложений: 1325

Комментарий: не указано

ПАРАМЕТРЫ ПРОВЕРКИ

Выполнена проверка с учетом редактирования: Да

Исключение элементов документа из проверки: Нет

Выполнено распознавание текста (OCR): Нет

Выполнена проверка с учетом структуры: Да

Модули поиска: СПС ГАРАНТ: нормативно-правовая документация, Переводные заимствования, IEEE, Цитирование, СМИ России и СНГ, Рувики, Шаблонные фразы, Патенты СССР, РФ, СНГ, Перефразирования по коллекции IEEE, Публикации eLIBRARY, Переводные заимствования по коллекции Гарант: аналитика, Кольцо вузов, ИПС Адилет, Публикации РГБ, СПС ГАРАНТ: аналитика, Переводные заимствования IEEE, Публикации РГБ (переводы и перефразирования), Перефразированные заимствования по коллекции Интернет в английском сегменте, Медицина, Сводная коллекция ЭБС, Переводные заимствования по коллекции Интернет в русском сегменте, Коллекция НБУ, Диссертации НББ, Интернет Плюс, Публикации eLIBRARY (переводы и перефразирования), Кольцо вузов (переводы и перефразирования), Перефразированные заимствования по коллекции Интернет в русском сегменте, Переводные заимствования по коллекции Интернет в английском сегменте, Перефразирования по СПС ГАРАНТ: аналитика, Собственная коллекция компании, Собственная коллекция (переводы и перефразирования)

ИСТОЧНИКИ

№	Доля в тексте	Доля в отчете	Источник	Актуален на	Модуль поиска	Комментарий
[01]	6,92%	1,66%	сПД801.zip/сПД801 Кайгородов С...	25 Июл 2023	Кольцо вузов (переводы и перефразирования)	
[02]	6,64%	0,72%	ISBN9785987045138.txt	26 Окт 2017	Кольцо вузов	
[03]	6,52%	0,95%	Недосекова, Елена Станиславовн... http://dlib.rsl.ru	01 Янв 2011	Публикации РГБ	
[04]	6,51%	0%	Правовое обеспечение национа...	27 Ноя 2017	Сводная коллекция ЭБС	
[05]	6,14%	3,63%	не указано	29 Сен 2022	Шаблонные фразы	
[06]	6,05%	2,95%	«Правовая защита в сфере инфо...	06 Мая 2025	Кольцо вузов (переводы и перефразирования)	
[07]	6,02%	0%	Правовое обеспечение национа...	20 Янв 2020	Сводная коллекция ЭБС	
[08]	6%	0,31%	Виноградов Б.В._ОНБсд-1701а	13 Дек 2023	Кольцо вузов	
[09]	5,76%	0%	Правовое обеспечение национа...	20 Дек 2016	Медицина	
[10]	5,69%	0%	сПД801.zip/сПД801 Кайгородов С...	25 Июл 2023	Кольцо вузов	
[11]	5,66%	0%	http://igpran.ru/prepare/a.person... http://igpran.ru	21 Фев 2022	Интернет Плюс	
[12]	5,66%	0%	http://igpran.ru/prepare/a.person... http://igpran.ru	30 Июн 2022	Интернет Плюс	
[13]	5,66%	0%	http://www.igpran.ru/prepare/a.p... http://igpran.ru	12 Янв 2020	Интернет Плюс	
[14]	5,64%	0%	ChebotarevaAA_diss.pdf http://xn--80afowig.xn--p1ai	18 Дек 2024	Интернет Плюс	
[15]	5,5%	0,21%	Чеботарева, Анна Александровн... http://dlib.rsl.ru	01 Янв 2017	Публикации РГБ	
[16]	5,26%	0,3%	Информационное право	19 Дек 2016	Медицина	
[17]	5,23%	0%	Куняев, Николай Николаевич Пр... http://dlib.rsl.ru	01 Янв 2010	Публикации РГБ	
[18]	5,21%	0%	Противодействие преступления... http://ivo.garant.ru	18 Мар 2023	Перефразирования по СПС ГАРАНТ: аналитика	
[19]	5,19%	0,21%	ОРГАНИЗАЦИОННОЕ И ПРАВОВО...	22 Фев 2017	Сводная коллекция ЭБС	
[20]	5,15%	0,03%	3.12.14. ДиссертацияКожухановР...	03 Дек 2014	Кольцо вузов	
[21]	5,08%	0%	Комментарий к Федеральному з... http://ivo.garant.ru	05 Июн 2021	СПС ГАРАНТ: аналитика	
[22]	4,98%	2,4%	Дубень, Андрей Кириллович Пра... http://dlib.rsl.ru	03 Апр 2025	Публикации РГБ (переводы и перефразирования)	
[23]	4,8%	1,46%	Kursovaya_IP	25 Дек 2023	Собственная коллекция (переводы и перефразирования)	

[24]	4,79%	0%	Комментарий к Федеральному з... http://ivo.garant.ru	30 Дек 2023	СПС ГАРАНТ: аналитика
[25]	4,79%	1,61%	Горбунов НКР антиплагиат	18 Июн 2024	Кольцо вузов (переводы и перефразирования)
[26]	4,56%	0%	Правовые основы информацион... http://ibooks.ru	09 Дек 2016	Сводная коллекция ЭБС
[27]	4,52%	0%	Полякова, Татьяна Анатольевна ... http://dlib.rsl.ru	01 Янв 2008	Публикации РГБ
[28]	4,39%	0%	Организационно-правовое обес...	20 Янв 2020	Сводная коллекция ЭБС
[29]	4,38%	0,45%	Горбунов НКР антиплагиат	18 Июн 2024	Кольцо вузов
[30]	4,36%	0,14%	Актуальные проблемы информа... https://book.ru	01 Янв 2019	Сводная коллекция ЭБС
[31]	4,32%	0%	Куликова С.А., Пешкова (Белогор... http://ivo.garant.ru	29 Авг 2020	СПС ГАРАНТ: аналитика
[32]	4,08%	0,13%	МД Слепцов 3	18 Мар 2025	Кольцо вузов
[33]	4,07%	0,27%	Глоссарий терминов в сфере ин... https://book.ru	01 Янв 2018	Сводная коллекция ЭБС
[34]	3,9%	0,31%	Информационные технологии в ... http://ivo.garant.ru	16 Ноя 2024	Перефразирования по СПС ГАРАНТ: аналитика
[35]	3,76%	1,59%	kursova(1).docx	29 Дек 2022	Собственная коллекция (переводы и перефразирования)
[36]	3,74%	1,57%	%D0%91%D0%B5%D1%80%D0%B... https://dspace.tltsu.ru	23 Июн 2025	Перефразированные заимствования по коллекции Интернет в русском сегменте
[37]	3,74%	0%	Противодействие преступления... http://ivo.garant.ru	18 Мар 2023	СПС ГАРАНТ: аналитика
[38]	3,65%	0%	Информационное право. Конспе...	19 Дек 2016	Медицина
[39]	3,61%	0%	ТАКТИКА СЛЕДСТВЕННОГО ОСМ...	08 Апр 2025	Публикации eLIBRARY
[40]	3,6%	0%	Информационное право (для бак... https://book.ru	01 Янв 2017	Сводная коллекция ЭБС
[41]	3,48%	0,29%	Федосин, Алексей Сергеевич За... http://dlib.rsl.ru	01 Янв 2009	Публикации РГБ
[42]	3,28%	0%	Основы информационного права	19 Дек 2016	Медицина
[43]	3,22%	0,27%	Дубень, Андрей Кириллович Пра... http://dlib.rsl.ru	01 Янв 2023	Публикации РГБ
[44]	3,22%	0%	%D0%94%D1%83%D0%B1%D0%B... http://igpran.ru	19 Ноя 2024	Интернет Плюс
[45]	3,18%	0%	Особенности правового регулир... https://dspace.tltsu.ru	15 Фев 2024	Перефразированные заимствования по коллекции Интернет в русском сегменте
[46]	3,14%	0%	Наделяева И.Е._ОНБсдо-1701а	21 Июн 2022	Кольцо вузов
[47]	3,1%	0,39%	«Правовая защита в сфере инфо...	06 Мая 2025	Кольцо вузов
[48]	3,05%	3,05%	Доктрина информационной безо... http://ivo.garant.ru	14 Окт 2000	СПС ГАРАНТ: нормативно-правовая документация
[49]	2,83%	1,04%	П. Н. Башлы, А. В. Бабаш, Е. К. Ба... http://dlib.rsl.ru	17 Фев 2014	Публикации РГБ (переводы и перефразирования)
[50]	2,83%	0,26%	Конфиденциальное делопроизв...	20 Дек 2016	Медицина
[51]	2,8%	0%	Правовые аспекты информацио... http://elibrary.ru	01 Янв 2021	Публикации eLIBRARY
[52]	2,76%	0,4%	Курсовая 2 курс ТГП	05 Мая 2025	Кольцо вузов (переводы и перефразирования)
[53]	2,7%	0,1%	Федеральный закон от 27.07.200... http://usd.iwn.sudrf.ru	29 Ноя 2021	СМИ России и СНГ
[54]	2,66%	0%	Семизорова, Екатерина Владими... http://dlib.rsl.ru	01 Янв 2007	Публикации РГБ
[55]	2,61%	0,36%	ОСНОВЫ ИНФОРМАЦИОННОЙ Б...	31 Мая 2025	Публикации eLIBRARY
[56]	2,61%	0%	Основы информационной безоп...	01 Июн 2025	Публикации eLIBRARY
					Перефразированные

[57]	2,61%	0%	Научная работа по предмету "П... https://infourok.ru	02 Июл 2025	заимствования по коллекции Интернет в русском сегменте
[58]	2,58%	0,07%	Информационные технологии в ... http://ivo.garant.ru	16 Ноя 2024	СПС ГАРАНТ: аналитика
[59]	2,57%	0,88%	РАХМОНЗОДА ДИЛШОДИ АЗИЗП...	19 Июн 2025	Кольцо вузов (переводы и перефразирования)
[60]	2,57%	0,59%	Информационная безопасность ... http://elibrary.ru	01 Янв 2021	Публикации eLIBRARY
[61]	2,55%	2,11%	Лихачев, Никита Александрович... http://dlib.rsl.ru	01 Янв 2024	Публикации РГБ (переводы и перефразирования)
[62]	2,4%	0%	Основы информационной безоп...	19 Дек 2016	Медицина
[63]	2,4%	0%	Курсовая итог на проверку.docx	25 Дек 2022	Собственная коллекция компании
[64]	2,39%	0,42%	Макаров, Олег Сергеевич Право... http://dlib.rsl.ru	01 Янв 2013	Публикации РГБ (переводы и перефразирования)
[65]	2,39%	0,02%	курсовая работа	28 Дек 2018	Собственная коллекция (переводы и перефразирования)
[66]	2,38%	0%	Колосович, Марина Сергеевна П... http://dlib.rsl.ru	01 Янв 2019	Публикации РГБ
[67]	2,16%	0%	Федеральный закон "Об информ... http://sanktpeterburg.bezformata.ru	24 Сен 2014	СМИ России и СНГ
[68]	2,16%	0%	Федеральный закон "Об информ... http://lenizdat.ru	24 Сен 2014	СМИ России и СНГ
[69]	2,13%	0%	Саранчук, Юрий Михайлович О... http://dlib.rsl.ru	01 Янв 2005	Публикации РГБ
[70]	2,06%	1,1%	Постановление Совета Федерац... http://ivo.garant.ru	19 Апр 2008	СПС ГАРАНТ: нормативно-правовая документация
[71]	2,04%	1,4%	Technical and Legal Principles of I... https://ieeexplore.ieee.org	01 Июл 2023	Переводные заимствования IEEE
[72]	2,01%	0%	Kursovaya_IP	25 Дек 2023	Собственная коллекция компании
[73]	1,96%	0%	Информационная безопасность ...	19 Дек 2016	Медицина
[74]	1,83%	0%	Агешкина Н.А., Соболева Ю.В., Хо...	07 Фев 2025	СПС ГАРАНТ: аналитика
[75]	1,8%	1,8%	Правовые основы защиты инфо...	05 Июл 2025	Публикации eLIBRARY (переводы и перефразирования)
[76]	1,73%	0,24%	Правовые аспекты защиты крит... http://elibrary.ru	01 Янв 2018	Публикации eLIBRARY
[77]	1,72%	0%	Право цифровой среды (монография... http://ivo.garant.ru	20 Авг 2022	СПС ГАРАНТ: аналитика
[78]	1,63%	0%	Совершенствование уголовно-п... http://diss.natlib.uz	21 Авг 2019	Коллекция НБУ
[79]	1,61%	0,33%	Экомир будущего глазами молод...	05 Июл 2025	Публикации eLIBRARY (переводы и перефразирования)
[80]	1,56%	0%	итог 23.01 — без источников	23 Янв 2020	Собственная коллекция компании
[81]	1,53%	0,04%	Постановление Пленума ВСРФ о ... http://journalist-virt.ru	29 Мая 2010	СМИ России и СНГ
[82]	1,5%	0%	Административное право Росси...	19 Дек 2016	Медицина
[83]	1,48%	0%	Григорян, Гарик Рафикович Мош... http://dlib.rsl.ru	01 Янв 2021	Публикации РГБ
[84]	1,46%	0,48%	Сухоруков, Артем Валерьевич П... http://dlib.rsl.ru	03 Апр 2025	Публикации РГБ (переводы и перефразирования)
[85]	1,43%	0%	%D0%95%D0%B3%D0%BE%D1%8... https://dspace.tltsu.ru	08 Апр 2025	Перефразированные заимствования по коллекции Интернет в русском сегменте
[86]	1,4%	0,13%	О защите критической информа... http://essentuki.bezformata.ru	02 Окт 2017	СМИ России и СНГ
[87]	1,39%	0%	Акимов Л.Ю., Андриченко Л.В., А... http://ivo.garant.ru	10 Дек 2016	СПС ГАРАНТ: аналитика
[88]	1,36%	0,34%	Болтанова Е.С., Здоровцева А.А., ... http://ivo.garant.ru	06 Мая 2017	СПС ГАРАНТ: аналитика
[89]	1,34%	0,52%	Курсовая 2	23 Ноя 2024	Собственная коллекция (переводы

					и перефразирования)	
[90]	1,3%	0%	Информационная безопасность ... http://elibrary.ru	27 Мая 2019	Публикации eLIBRARY	
[91]	1,24%	0%	Гражданско-правовая охрана ли... http://diss.natlib.uz	02 Сен 2014	Коллекция НБУ	
[92]	1,23%	0,33%	Курсовая 2	23 Ноя 2024	Собственная коллекция компании	
[93]	1,23%	0%	2022-VKR-BA-AlekseevaPI-18707	09 Июн 2022	Кольцо вузов	
[94]	1,21%	0%	Обеспечение защиты прав и св... http://penza.ru	02 Дек 2009	СМИ России и СНГ	
[95]	1,21%	0%	Воробьев Н.И., Галкин В.А., Моке...	27 Мар 2025	Перефразирования по СПС ГАРАНТ: аналитика	
[96]	1,19%	0%	АКТУАЛЬНЫЕ ПРАВОВЫЕ ПРОБЛ... http://elibrary.ru	01 Янв 2024	Публикации eLIBRARY (переводы и перефразирования)	
[97]	1,19%	0%	919641051.pdf https://publications.hse.ru	14 Мая 2025	Перефразированные заимствования по коллекции Интернет в русском сегменте	
[98]	1,17%	0,03%	Правовые_основы_компенсацио...	22 Апр 2025	Кольцо вузов	
[99]	1,15%	0,84%	Федеральный закон от 26 июля ... http://ivo.garant.ru	10 Июл 2023	СПС ГАРАНТ: нормативно-правовая документация	
[100]	1,15%	0%	роследняя Курсовая	06 Мар 2022	Собственная коллекция компании	
[101]	1,15%	0%	kursovaya_na_proverku.docx	07 Дек 2022	Собственная коллекция компании	
[102]	1,15%	0%	kurs (1)-2	27 Дек 2023	Собственная коллекция компании	
[103]	1,11%	0%	Итоговый вариант. Курсовая ра...	18 Дек 2021	Собственная коллекция компании	
[104]	1,06%	0%	Журналистские расследования https://ru.ruwiki.ru	раньше 2011	Рувики	
[105]	0,95%	0%	Правовые проблемы построени...	11 Ноя 2016	Диссертации НББ	
[106]	0,94%	0%	Право на анонимность https://ru.ruwiki.ru	раньше 2011	Рувики	Источник исключен. Причина: Маленький процент пересечения.
[107]	0,94%	0%	Постановление Совета Федерац... http://ivo.garant.ru	12 Июн 2010	СПС ГАРАНТ: нормативно-правовая документация	Источник исключен. Причина: Маленький процент пересечения.
[108]	0,91%	0%	https://www.psi.perm.ru/images/l... https://psi.perm.ru	26 Мая 2025	Интернет Плюс	Источник исключен. Причина: Маленький процент пересечения.
[109]	0,88%	0%	Теоретико-практические особен... http://diss.natlib.uz	12 Фев 2019	Коллекция НБУ	
[110]	0,87%	0%	ПРОЕКТ ПОСТАНОВЛЕНИЯ "Об ут... http://krasnokamensk.bezformata.ru	12 Ноя 2015	СМИ России и СНГ	Источник исключен. Причина: Маленький процент пересечения.
[111]	0,86%	0,22%	АСПЕКТЫ И УГРОЗЫ ИНФОРМАЦ... http://elibrary.ru	01 Янв 2022	Публикации eLIBRARY	
[112]	0,86%	0%	Анализ положений Доктрины ин... http://securitylab.ru	10 Фев 2017	СМИ России и СНГ	Источник исключен. Причина: Маленький процент пересечения.
[113]	0,86%	0%	%D0%94%D1%83%D0%B1%D0%B... http://igpran.ru	19 Ноя 2024	Перефразированные заимствования по коллекции Интернет в русском сегменте	
[114]	0,86%	0%	karataeva_a_-_problemy-v-deyatel...	09 Мая 2021	Кольцо вузов (переводы и перефразирования)	
[115]	0,84%	0%	Андросов М.В., Бажайкин А.Л., Б... http://ivo.garant.ru	16 Янв 2016	Перефразирования по СПС ГАРАНТ: аналитика	
[116]	0,81%	0,81%	Курсовая Насти	01 Дек 2024	Собственная коллекция (переводы и перефразирования)	
[117]	0,8%	0%	Персональные данные https://ru.ruwiki.ru	раньше 2011	Рувики	
[118]	0,77%	0,77%	Критическая информационная и... http://ivo.garant.ru	23 Июл 2022	Переводные заимствования по коллекции Гарант: аналитика	
[119]	0,76%	0,12%	Security of critical information inf... https://tadviser.com	14 Июн 2025	Переводные заимствования по коллекции Интернет в английском сегменте	

[120]	0,75%	0%	Дубень, Андрей Кириллович Пра... http://dlib.rsl.ru	01 Янв 2023	Публикации РГБ (переводы и перефразирования)	Источник исключен. Причина: Маленький процент пересечения.
[121]	0,73%	0%	Основные права и свободы https://ru.ruwiki.ru	раньше 2011	Рувики	Источник исключен. Причина: Маленький процент пересечения.
[122]	0,72%	0,72%	Концепция информационной бе... http://ivo.garant.ru	05 Июл 2022	СПС ГАРАНТ: нормативно-правовая документация	
[123]	0,71%	0,14%	Что такое информационная безо... http://barnaul.bezformata.ru	19 Фев 2018	СМИ России и СНГ	
[124]	0,7%	0%	Обеспечение права граждан на ...	05 Июл 2025	Публикации eLIBRARY (переводы и перефразирования)	
[125]	0,69%	0%	Неправомерное завладение ком...	16 Янв 2020	Диссертации НББ	Источник исключен. Причина: Маленький процент пересечения.
[126]	0,65%	0%	Курсовая работа ИП.docx	25 Дек 2021	Собственная коллекция компании	Источник исключен. Причина: Маленький процент пересечения.
[127]	0,62%	0%	Международные стандарты в об... http://diss.natlib.uz	02 Сен 2014	Коллекция НБУ	Источник исключен. Причина: Маленький процент пересечения.
[128]	0,61%	0,48%	kursovaya 999	27 Дек 2019	Собственная коллекция (переводы и перефразирования)	
[129]	0,59%	0,47%	Токолов, Александр Владимиров... http://dlib.rsl.ru	01 Янв 2022	Публикации РГБ (переводы и перефразирования)	
[130]	0,59%	0%	Курсовая ИП А.С.Водянов	17 Янв 2022	Собственная коллекция компании	Источник исключен. Причина: Маленький процент пересечения.
[131]	0,56%	0%	Организация аппаратно-програ... http://diss.natlib.uz	02 Сен 2014	Коллекция НБУ	Источник исключен. Причина: Маленький процент пересечения.
[132]	0,53%	0%	Постановление Совета Федерац... http://ivo.garant.ru	04 Апр 2009	СПС ГАРАНТ: нормативно-правовая документация	Источник исключен. Причина: Маленький процент пересечения.
[133]	0,53%	0%	Синтез полифункциональных со...	11 Ноя 2016	Диссертации НББ	Источник исключен. Причина: Маленький процент пересечения.
[134]	0,5%	0,5%	Соглашение между Правительст... http://ivo.garant.ru	22 Авг 2022	СПС ГАРАНТ: нормативно-правовая документация	
[135]	0,5%	0%	Распоряжение Правительства Р... http://ivo.garant.ru	28 Мар 2022	СПС ГАРАНТ: нормативно-правовая документация	
[136]	0,5%	0%	Распоряжение Правительства Р... http://ivo.garant.ru	24 Сен 2020	СПС ГАРАНТ: нормативно-правовая документация	
[137]	0,5%	0%	Под кибератаки предложена нов... http://banki.ru	07 Дек 2016	СМИ России и СНГ	
[138]	0,5%	0%	Интернет-преступность в России https://ru.ruwiki.ru	раньше 2011	Рувики	
[139]	0,5%	0%	Преступления в сфере информа... https://ru.ruwiki.ru	раньше 2011	Рувики	
[140]	0,5%	0%	Штодина, Дарья Дмитриевна Ме... http://dlib.rsl.ru	20 Сен 2024	Публикации РГБ (переводы и перефразирования)	
[141]	0,48%	0,36%	948400dd16fdd527cd2c43d2eb49... https://magazine.neftegaz.ru	12 Авг 2024	Переводные заимствования по коллекции Интернет в русском сегменте	
[142]	0,44%	0%	Обеспечение баланса частнопр... http://ivo.garant.ru	30 Мар 2024	СПС ГАРАНТ: аналитика	Источник исключен. Причина: Маленький процент пересечения.
[143]	0,44%	0%	disGinz.pdf https://special.rpa-mu.ru	26 Дек 2024	Перефразированные заимствования по коллекции Интернет в русском сегменте	
[144]	0,43%	0%	Использование и защита конфи... http://diss.natlib.uz	12 Фев 2019	Коллекция НБУ	Источник исключен. Причина: Маленький процент пересечения.
[145]	0,42%	0%	АСПЕКТЫ И УГРОЗЫ ИНФОРМАЦ... http://elibrary.ru	01 Янв 2022	Публикации eLIBRARY (переводы и перефразирования)	Источник исключен. Причина: Маленький процент пересечения.
[146]	0,41%	0%	1044081758.pdf https://publications.hse.ru	08 Мая 2025	Интернет Плюс	Источник исключен. Причина: Маленький процент пересечения.
[147]	0,38%	0%	Ефремов, Алексей Александрови... http://dlib.rsl.ru	01 Янв 2020	Публикации РГБ (переводы и перефразирования)	Источник исключен. Причина: Маленький процент пересечения.
[148]	0,38%	0%	https://studfile.net/preview/17112... https://studfile.net	28 Янв 2024	Переводные заимствования по коллекции Интернет в русском сегменте	Источник исключен. Причина: Маленький процент пересечения.
[149]	0,37%	0%	Международно-правовое сотруд...	11 Ноя 2016	Диссертации НББ	Источник исключен. Причина: Маленький процент пересечения.

[150]	0,34%	0%	Болтанова Е.С., Здоровцева А.А., ... http://ivo.garant.ru	06 Мая 2017	Перефразирования по СПС ГАРАНТ: аналитика	Источник исключен. Причина: Маленький процент пересечения.
[151]	0,34%	0%	ФИПС - Федеральное государств... http://www1.fips.ru	03 Ноя 2016	Патенты СССР, РФ, СНГ	Источник исключен. Причина: Маленький процент пересечения.
[152]	0,34%	0%	ФИПС - Федеральное государств... http://www1.fips.ru	03 Ноя 2016	Патенты СССР, РФ, СНГ	Источник исключен. Причина: Маленький процент пересечения.
[153]	0,34%	0%	https://science.vvsu.ru/files/C869... https://science.vvsu.ru	29 Дек 2023	Перефразированные заимствования по коллекции Интернет в русском сегменте	Источник исключен. Причина: Маленький процент пересечения.
[154]	0,34%	0%	Решение Екатеринбургской горо... http://ivo.garant.ru	08 Июн 2010	СПС ГАРАНТ: нормативно-правовая документация	Источник исключен. Причина: Маленький процент пересечения.
[155]	0,34%	0%	О Концепции информационной ... http://adilet.zan.kz	21 Янв 2016	ИПС Адилет	Источник исключен. Причина: Маленький процент пересечения.
[156]	0,33%	0%	Глобальное информационное пр... http://diss.natlib.uz	03 Мар 2017	Коллекция НБУ	Источник исключен. Причина: Маленький процент пересечения.
[157]	0,33%	0%	Об утверждении Инструкции по ... http://adilet.zan.kz	21 Янв 2016	ИПС Адилет	Источник исключен. Причина: Маленький процент пересечения.
[158]	0,3%	0%	Административно-правовое обе...	11 Ноя 2016	Диссертации НББ	Источник исключен. Причина: Маленький процент пересечения.
[159]	0,23%	0%	Уголовная ответственность за н...	11 Ноя 2016	Диссертации НББ	Источник исключен. Причина: Маленький процент пересечения.
[160]	0,21%	0%	Информационный посредник https://ru.ruwiki.ru	раньше 2011	Рувики	Источник исключен. Причина: Маленький процент пересечения.
[161]	0,21%	0%	Критически важные объекты и к... http://ibooks.ru	09 Дек 2016	Сводная коллекция ЭБС	Источник исключен. Причина: Маленький процент пересечения.
[162]	0,21%	0%	Свобода информации https://ru.ruwiki.ru	раньше 2011	Рувики	Источник исключен. Причина: Маленький процент пересечения.
[163]	0,2%	0%	Правовые основы защиты прав ... http://diss.natlib.uz	02 Сен 2014	Коллекция НБУ	Источник исключен. Причина: Маленький процент пересечения.
[164]	0,15%	0%	не указано	13 Янв 2022	Цитирование	Источник исключен. Причина: Маленький процент пересечения.
[165]	0,13%	0%	ФИПС - Федеральное государств... http://www1.fips.ru	03 Ноя 2016	Патенты СССР, РФ, СНГ	Источник исключен. Причина: Маленький процент пересечения.

Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

Юридический факультет

Кафедра информационного, гражданского права
и правового обеспечения инновационной деятельности (ИГПиПОИД)

Правовое обеспечение информационной безопасности

Курсовая работа
по дисциплине «Информационное право»

Студент гр. з-093П5-5
Гасанов Руслан Нураддин оглы

Руководитель
Канд. юрид. наук
Афанасьева Екатерина
Нодариевна

Томск 2025 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современном информационном обществе вопросы обеспечения информационной безопасности приобретают особую актуальность и значимость. Стремительное развитие информационных технологий, цифровизация всех сфер жизнедеятельности общества и государства, а также возрастающие киберугрозы обуславливают необходимость создания эффективной системы правового регулирования информационной безопасности. Актуальность темы исследования определяется тем, что в условиях цифровой трансформации общества информация становится не только ценным ресурсом, но и объектом повышенной опасности, требующим надежной правовой защиты.

Правовое обеспечение информационной безопасности представляет собой комплексный институт, включающий нормы различных отраслей права, направленные на защиту информации, информационных систем и информационной инфраструктуры от внешних и внутренних угроз. Особую значимость данная проблематика приобретает в контексте обеспечения национальной безопасности Российской Федерации, защиты конституционных прав граждан на неприкосновенность частной жизни, личную и семейную тайну, а также обеспечения устойчивого функционирования критической информационной инфраструктуры.

Степень разработанности проблемы в научной литературе характеризуется наличием значительного количества исследований, посвященных различным аспектам правового обеспечения информационной безопасности. Теоретические основы информационной безопасности, ее правовые аспекты рассматриваются в работах Т.А. Поляковой, Г.Г. Камаловой, Л.В. Магдиловой. Конституционные аспекты обеспечения информационной безопасности исследуются в трудах Д.М. Зуенко, Е.А. Осадчука, М.К. Водопьяновой. Вопросы международного опыта правового регулирования информационной безопасности анализируются в работах

Э.В. Горяна, А.К. Дубеня. Проблемы противодействия киберугрозам рассматриваются в исследованиях Ю.Н. Сосновской, Е.О. Бондаря, Бакытбек Кызы Ай, Ж.И. Калбаева. Однако, несмотря на значительное количество научных работ, многие аспекты правового обеспечения информационной безопасности требуют дальнейшего исследования и систематизации.

Целью настоящей работы является комплексное исследование теоретических и практических аспектов правового обеспечения информационной безопасности, выявление проблем правового регулирования в данной сфере и разработка предложений по его совершенствованию.

Для достижения поставленной цели необходимо решить следующие задачи:

- исследовать понятие и сущность информационной безопасности в правовом аспекте;

- проанализировать нормативно-правовое регулирование информационной безопасности в Российской Федерации;

- изучить международный опыт правового регулирования информационной безопасности;

- рассмотреть механизмы правовой защиты информационной безопасности;

- выявить проблемы правоприменительной практики в сфере информационной безопасности;

- разработать предложения по совершенствованию правового регулирования информационной безопасности.

Объектом исследования являются общественные отношения, возникающие в процессе правового обеспечения информационной безопасности.

Предметом исследования выступают нормативные правовые акты, регулирующие вопросы обеспечения информационной безопасности, а также научные концепции и подходы к пониманию сущности и содержания правового обеспечения информационной безопасности.

Методологическую основу исследования составляют общенаучные методы познания (анализ, синтез, индукция, дедукция, системный подход) и специально-юридические методы (формально-юридический, сравнительно-правовой, историко-правовой).

Теоретическую базу исследования составляют труды отечественных и зарубежных ученых в области информационного права, информационной безопасности, конституционного права, административного права и других отраслей юридической науки.

Практическая значимость работы заключается в возможности использования ее результатов в процессе совершенствования законодательства в сфере информационной безопасности, а также в правоприменительной практике органов государственной власти, осуществляющих деятельность по обеспечению информационной безопасности. Кроме того, материалы исследования могут быть использованы в учебном процессе при преподавании дисциплин информационно-правового цикла.

Глава 1. Теоретико-правовые основы обеспечения информационной безопасности

1.1 Понятие и сущность информационной безопасности в правовом аспекте

Информационная безопасность в современном мире представляет собой многоаспектное явление, требующее комплексного правового регулирования. Для полноценного понимания сущности информационной безопасности в правовом аспекте необходимо проанализировать существующие подходы к определению данного понятия, выявить его ключевые элементы и сформулировать авторскую позицию по данному вопросу.

В российском законодательстве отсутствует единое легальное определение понятия "информационная безопасность". Однако в Федеральном законе "Об информации, информационных технологиях и о защите информации" закреплены основные принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации, которые косвенно характеризуют сущность информационной безопасности [3]. Данный нормативный правовой акт устанавливает, что правовое регулирование отношений в сфере информации основывается на принципах свободы поиска, получения, передачи, производства и распространения информации любым законным способом; установления ограничений доступа к информации только федеральными законами; открытости информации о деятельности государственных органов и органов местного самоуправления; обеспечения безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации.

Конституция Российской Федерации, хотя и не содержит прямого упоминания информационной безопасности, закрепляет ряд фундаментальных

прав и свобод, связанных с информационной сферой, которые подлежат правовой защите. В частности, статья 23 гарантирует право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, а также тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений [1]. Статья 24 устанавливает запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. Статья 29 закрепляет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Таким образом, конституционные нормы формируют правовую основу для обеспечения информационной безопасности личности.

В научной литературе существуют различные подходы к определению понятия "информационная безопасность". Т.А. Полякова и Г.Г. Камалова рассматривают информационную безопасность как состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства [8, с. 114]. Данный подход акцентирует внимание на триаде субъектов, чьи интересы подлежат защите в информационной сфере.

Л.В. Магдилова определяет информационную безопасность как состояние защищенности информационной среды, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства [6, с. 213]. В данном определении акцент делается на защищенности информационной среды как таковой, что представляется несколько узким подходом, не учитывающим всех аспектов информационной безопасности.

М.К. Водопьянова, исследуя конституционные гарантии приватности и киберугрозы, рассматривает информационную безопасность через призму защиты критической информационной инфраструктуры и определяет ее как состояние защищенности информационной инфраструктуры от внешних и внутренних угроз, при котором обеспечивается ее устойчивое функционирование в условиях

возможного негативного информационного воздействия [2, с. 33]. Данный подход акцентирует внимание на технологическом аспекте информационной безопасности.

Зарубежные исследователи также предлагают различные подходы к определению информационной безопасности. Э.В. Горян, анализируя опыт правового регулирования информационной безопасности в Таиланде, отмечает, что в зарубежной практике информационная безопасность часто рассматривается через призму кибербезопасности и определяется как состояние защищенности информационных систем и сетей от несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения информации [3, с. 110]. Данный подход также акцентирует внимание на технологическом аспекте информационной безопасности.

А.К. Дубень, исследуя международный опыт правового регулирования информационной безопасности, отмечает, что в международной практике информационная безопасность рассматривается как комплексное понятие, включающее в себя защиту информации, информационных систем и информационной инфраструктуры от внешних и внутренних угроз, а также обеспечение информационного суверенитета государства [4, с. 255]. Данный подход представляется наиболее комплексным, учитывающим различные аспекты информационной безопасности.

Анализируя различные подходы к определению понятия "информационная безопасность", можно выделить следующие ключевые элементы данного понятия:

1. Состояние защищенности информации, информационных систем и информационной инфраструктуры от внешних и внутренних угроз.

2. Обеспечение конфиденциальности, целостности и доступности информации.

3. Защита интересов личности, общества и государства в информационной сфере.

4. Обеспечение информационного суверенитета государства.

5. Противодействие информационным угрозам и вызовам.

На основе анализа существующих подходов и выделенных ключевых элементов можно сформулировать следующее определение: информационная безопасность в правовом аспекте представляет собой состояние защищенности информации, информационных систем и информационной инфраструктуры от внешних и внутренних угроз, при котором обеспечивается конфиденциальность, целостность и доступность информации, защита интересов личности, общества и государства в информационной сфере, а также информационный суверенитет государства.

Правовое обеспечение информационной безопасности представляет собой систему правовых норм и институтов, направленных на регулирование общественных отношений в сфере защиты информации, информационных систем и информационной инфраструктуры от внешних и внутренних угроз. Данная система включает в себя нормы различных отраслей права: конституционного, административного, уголовного, гражданского, информационного и др.

Правовое обеспечение информационной безопасности осуществляется на различных уровнях: международном, региональном, национальном и локальном. На международном уровне формируются общие принципы и стандарты обеспечения информационной безопасности, которые затем имплементируются в национальное законодательство государств. На национальном уровне создается система нормативных правовых актов, регулирующих различные аспекты информационной безопасности. На локальном уровне разрабатываются и принимаются локальные нормативные акты, регулирующие вопросы обеспечения информационной безопасности в конкретных организациях.

Таким образом, информационная безопасность в правовом аспекте представляет собой комплексное понятие, включающее в себя различные элементы и аспекты, требующие правового регулирования. Эффективное правовое

обеспечение информационной безопасности возможно только при комплексном подходе, учитывающем интересы личности, общества и государства в информационной сфере, а также современные вызовы и угрозы в данной сфере.

1.2 Нормативно-правовое регулирование информационной безопасности в РФ

Нормативно-правовое регулирование информационной безопасности в Российской Федерации представляет собой многоуровневую систему правовых актов, формирующих комплексный механизм защиты информации, информационных систем и информационной инфраструктуры. Данная система включает в себя нормативные правовые акты различной юридической силы, начиная от Конституции РФ и заканчивая ведомственными актами и локальными нормативными документами.

Фундаментальной правовой основой обеспечения информационной безопасности в России является Конституция Российской Федерации, которая закрепляет базовые права и свободы граждан в информационной сфере. Статья 23 Конституции РФ гарантирует право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, а также тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений [1]. Статья 24 устанавливает запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. Эти конституционные положения формируют правовую основу для защиты информационных прав личности и определяют границы государственного вмешательства в информационную сферу.

Важнейшим элементом системы нормативно-правового регулирования информационной безопасности является Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации", который устанавливает основные принципы правового регулирования отношений

в сфере информации, определяет правовой режим информации различных категорий, регламентирует вопросы создания и эксплуатации информационных систем, а также устанавливает требования к защите информации [3]. Данный закон является базовым нормативным актом в сфере информационной безопасности и создает правовую основу для принятия других нормативных правовых актов в данной сфере.

Особое место в системе нормативно-правового регулирования информационной безопасности занимает Федеральный закон от 27 июля 2006 г. № 152-ФЗ "О персональных данных", который регулирует отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов РФ, иными государственными органами, органами местного самоуправления, юридическими и физическими лицами [4]. Данный закон устанавливает требования к обработке персональных данных, определяет права субъектов персональных данных, а также обязанности операторов персональных данных по обеспечению их безопасности.

Значимым элементом системы нормативно-правового регулирования информационной безопасности является Федеральный закон от 26 июля 2017 г. № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации", который устанавливает организационные и правовые основы обеспечения безопасности критической информационной инфраструктуры РФ в целях ее устойчивого функционирования при проведении в отношении нее компьютерных атак [5]. Данный закон определяет полномочия государственных органов в области обеспечения безопасности критической информационной инфраструктуры, а также права, обязанности и ответственность субъектов критической информационной инфраструктуры.

Т.А. Полякова и Г.Г. Камалова отмечают, что принятие Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" стало важным шагом в развитии системы правового обеспечения

информационной безопасности, поскольку данный закон создал правовую основу для защиты наиболее важных информационных систем и сетей, нарушение функционирования которых может привести к серьезным последствиям для национальной безопасности [8, с. 116].

Важную роль в системе нормативно-правового регулирования информационной безопасности играет Закон РФ от 5 марта 1992 г. № 2446-1 "О безопасности", который определяет основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством РФ [2]. Данный закон устанавливает полномочия и функции федеральных органов государственной власти, органов государственной власти субъектов РФ, органов местного самоуправления в области обеспечения безопасности, а также статус Совета Безопасности РФ.

Помимо федеральных законов, важное место в системе нормативно-правового регулирования информационной безопасности занимают подзаконные нормативные правовые акты, в частности, указы Президента РФ и постановления Правительства РФ. Среди них особое значение имеет Указ Президента РФ от 5 декабря 2016 г. № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации", который определяет стратегические цели и основные направления обеспечения информационной безопасности РФ, а также систему обеспечения информационной безопасности.

Л.В. Магдилова подчеркивает, что Доктрина информационной безопасности РФ является документом стратегического планирования, который определяет национальные интересы в информационной сфере, основные информационные угрозы и стратегические цели обеспечения информационной безопасности [6, с. 215]. Данный документ формирует основу для разработки и реализации государственной политики в сфере обеспечения информационной безопасности.

Важным элементом системы нормативно-правового регулирования информационной безопасности являются также ведомственные нормативные правовые акты, принимаемые федеральными органами исполнительной власти, осуществляющими регулирование в сфере информационной безопасности. К таким органам относятся, в частности, Федеральная служба по техническому и экспортному контролю (ФСТЭК России) и Федеральная служба безопасности РФ (ФСБ России).

Д.М. Зуенко и Е.А. Осадчук отмечают, что ведомственные нормативные правовые акты играют важную роль в системе нормативно-правового регулирования информационной безопасности, поскольку они детализируют требования федеральных законов и подзаконных актов, а также устанавливают конкретные технические и организационные меры по обеспечению информационной безопасности [5, с. 479].

Анализируя современное состояние нормативно-правовой базы РФ в сфере информационной безопасности, можно выделить следующие ее особенности:

1. Комплексный характер правового регулирования, обусловленный многоаспектностью информационной безопасности как объекта правового регулирования.

2. Многоуровневая структура нормативно-правовой базы, включающая в себя нормативные правовые акты различной юридической силы.

3. Динамичность развития правового регулирования, обусловленная быстрыми темпами развития информационных технологий и появлением новых информационных угроз.

4. Сочетание публично-правовых и частноправовых методов регулирования, что обусловлено необходимостью защиты как публичных, так и частных интересов в информационной сфере.

5. Наличие специализированных нормативных правовых актов, регулирующих отдельные аспекты информационной безопасности (защита

персональных данных, безопасность критической информационной инфраструктуры и др.).

Ю.Н. Сосновская и Е.О. Бондарь, исследуя вопросы административно-правового регулирования противодействия киберугрозам, отмечают, что современная нормативно-правовая база РФ в сфере информационной безопасности в целом соответствует международным стандартам и позволяет эффективно противодействовать основным информационным угрозам [9]. Однако, по мнению авторов, существуют определенные пробелы и коллизии в правовом регулировании, которые требуют устранения.

Таким образом, нормативно-правовое регулирование информационной безопасности в Российской Федерации представляет собой сложную многоуровневую систему правовых актов, которая постоянно развивается и совершенствуется в соответствии с изменяющимися условиями информационной среды и появлением новых информационных угроз. Эффективность данной системы зависит от согласованности и непротиворечивости нормативных правовых актов различного уровня, а также от их соответствия современным вызовам и угрозам в информационной сфере.

1.3 Международный опыт правового регулирования информационной безопасности

В условиях глобализации информационного пространства и трансграничного характера киберугроз особую значимость приобретает изучение международного опыта правового регулирования информационной безопасности. Анализ зарубежных моделей правового обеспечения информационной безопасности позволяет выявить наиболее эффективные подходы и механизмы, которые могут быть адаптированы к российским условиям. Международный опыт демонстрирует разнообразие подходов к правовому регулированию данной сферы,

обусловленное различиями в правовых системах, уровне технологического развития и национальных приоритетах в области информационной безопасности.

Соединенные Штаты Америки традиционно занимают лидирующие позиции в сфере развития информационных технологий и правового регулирования информационной безопасности.[75] Правовая система США в данной области характеризуется децентрализованным подходом и сочетанием федерального законодательства с законодательством штатов. Ключевыми федеральными законами являются Computer Fraud and Abuse Act (CFAA), Federal Information Security Management Act (FISMA), Cybersecurity Information Sharing Act (CISA) и Cybersecurity Enhancement Act. Особенностью американской модели является активное взаимодействие государственного и частного секторов в обеспечении информационной безопасности, что реализуется через механизмы государственно-частного партнерства и обмена информацией о киберугрозах [4, с. 255].

Европейский Союз реализует комплексный подход к правовому регулированию информационной безопасности, основанный на гармонизации законодательства государств-членов. Центральное место в европейской системе правового регулирования занимает Общий регламент по защите данных (General Data Protection Regulation, GDPR), вступивший в силу в 2018 году. Данный документ устанавливает единые правила обработки персональных данных на территории ЕС и предусматривает значительные штрафы за их нарушение. Другим важным элементом европейской системы является Директива о безопасности сетевых и информационных систем (NIS Directive), которая устанавливает требования к обеспечению кибербезопасности критической инфраструктуры и цифровых услуг [8, с. 118].

Китайская Народная Республика демонстрирует централизованный подход к правовому регулированию информационной безопасности, основанный на концепции "кибернетического суверенитета". Закон о кибербезопасности КНР, принятый в 2017 году, устанавливает жесткие требования к операторам

критической информационной инфраструктуры, включая обязательную локализацию данных и проверку безопасности сетевого оборудования. Особенностью китайской модели является активное государственное регулирование интернет-пространства и приоритет национальной безопасности над частными интересами [7, с. 35].

Анализируя международный опыт правового регулирования информационной безопасности, можно выделить несколько основных моделей (см. Таблицу 1).

Таблица 1 - Сравнительный анализ моделей правового регулирования информационной безопасности в различных странах

Страна/регион	Ключевые нормативные акты	Особенности правового регулирования	Приоритетные направления защиты
США	CFAA, FISMA, CISA, Cybersecurity Enhancement Act	Децентрализованный подход, государственно-частное партнерство	Критическая инфраструктура, государственные информационные системы
Европейский Союз	GDPR, NIS Directive, Cybersecurity Act	Гармонизация законодательства, баланс безопасности и прав человека	Персональные данные, критическая инфраструктура, цифровые услуги
Китай	Закон о кибербезопасности, Закон о защите персональных данных	Централизованный подход, концепция "кибернетического суверенитета"	Национальная безопасность, контроль информационного пространства
Япония	Основной закон кибербезопасности, Закон о защите персональной информации	Стратегический подход, акцент на технологические решения	Критическая инфраструктура, персональные данные, интеллектуальная собственность
Сингапур	Закон о кибербезопасности, Закон о защите персональных данных	Комплексный подход, развитие цифровой экономики	"Умный город", электронное правительство, финансовый сектор
Израиль	Резолюция о продвижении	Интеграция военных и гражданских	Критическая инфраструктура,

	национальных возможностей в киберпространстве	технологий, образовательные программы	военные системы, инновационные технологии

Составлено автором на основе [6]

Особый интерес представляет опыт Сингапура, который реализует комплексную стратегию развития "умного города" с интегрированной системой обеспечения информационной безопасности. Закон о кибербезопасности Сингапура, принятый в 2018 году, устанавливает обязательные требования к операторам критической информационной инфраструктуры и предусматривает создание национальной системы реагирования на киберинциденты. Сингапурская модель характеризуется сбалансированным подходом, сочетающим жесткое регулирование критической инфраструктуры с гибкими механизмами поддержки инноваций в сфере кибербезопасности [4, с. 256].

Израиль демонстрирует уникальный подход к обеспечению информационной безопасности, основанный на интеграции военных и гражданских технологий. Национальное киберуправление Израиля координирует деятельность государственных органов и частного сектора в сфере кибербезопасности, а также реализует образовательные программы по подготовке специалистов. Израильская модель отличается высокой степенью адаптивности к новым угрозам и активным развитием инновационных технологий в сфере информационной безопасности [9].

Динамика развития законодательства об информационной безопасности в различных странах демонстрирует общую тенденцию к усилению правового регулирования в ответ на растущие киберугрозы (см. Рисунок 1).

Составлено автором на основе [9]

Рисунок 1 - Динамика развития законодательства об информационной безопасности (индекс комплексности правового регулирования, 2015-2024 гг.)

Представленная диаграмма отражает рост комплексности правового регулирования информационной безопасности в ведущих странах мира за последнее десятилетие. Наиболее интенсивный рост наблюдается в Европейском Союзе после принятия GDPR и в Китае после внедрения концепции "кибернетического суверенитета". Россия демонстрирует устойчивый рост показателя, что свидетельствует о последовательном развитии нормативно-правовой базы в сфере информационной безопасности.

Анализируя международный опыт, можно выделить следующие перспективные направления развития правового регулирования информационной безопасности, которые могут быть адаптированы к российским условиям:

1. Развитие механизмов государственно-частного партнерства в сфере обеспечения информационной безопасности, включая создание платформ для обмена информацией о киберугрозах между государственными органами и частным сектором.

2. Совершенствование правового регулирования трансграничной передачи данных с учетом баланса между обеспечением национальной безопасности и интеграцией в глобальное информационное пространство.

3. Разработка специализированных правовых механизмов защиты критической информационной инфраструктуры с учетом отраслевой специфики и уровня критичности объектов.

4. Развитие правовых механизмов международного сотрудничества в сфере противодействия киберпреступности и кибертерроризму, включая гармонизацию национального законодательства с международными стандартами.

5. Совершенствование правового регулирования ответственности за нарушения в сфере информационной безопасности, включая дифференциацию ответственности в зависимости от характера и последствий нарушений.

Э.В. Горян, анализируя опыт правового регулирования информационной безопасности в странах Юго-Восточной Азии, отмечает, что эффективность правового регулирования в данной сфере зависит не только от наличия соответствующих нормативных актов, но и от создания действенных механизмов их реализации, включая специализированные органы по обеспечению кибербезопасности и программы повышения осведомленности населения [3, с. 112].

Таким образом, международный опыт правового регулирования информационной безопасности демонстрирует разнообразие подходов и моделей, обусловленное национальными особенностями и приоритетами. При этом можно выделить общие тенденции, характерные для большинства развитых стран: усиление правового регулирования в ответ на растущие киберугрозы, развитие специализированного законодательства по защите критической информационной инфраструктуры, совершенствование механизмов защиты персональных данных, а также развитие международного сотрудничества в сфере информационной безопасности.

Глава 2. Практические аспекты правового обеспечения информационной безопасности

2.1 Механизмы правовой защиты информационной безопасности

В современных условиях цифровизации общества и государства механизмы правовой защиты информационной безопасности приобретают особую значимость. Под механизмами правовой защиты информационной безопасности следует понимать совокупность правовых средств и инструментов, направленных на предотвращение, выявление и пресечение нарушений в информационной сфере, а также восстановление нарушенных прав и привлечение виновных лиц к ответственности. Данные механизмы формируют целостную систему, обеспечивающую реализацию правовых норм в области информационной безопасности.

Конституционно-правовые механизмы защиты информационной безопасности основываются на фундаментальных положениях Конституции РФ и включают в себя судебную защиту прав и свобод в информационной сфере, деятельность Конституционного Суда РФ по проверке конституционности законов и иных нормативных правовых актов в данной области, а также институт Уполномоченного по правам человека. Особое значение имеет конституционное право на судебную защиту, которое позволяет гражданам и организациям оспаривать в судебном порядке решения и действия (бездействие) органов государственной власти, нарушающие их права в информационной сфере [1].

Административно-правовые механизмы защиты информационной безопасности реализуются через систему органов исполнительной власти, осуществляющих контрольно-надзорные функции в данной сфере. Ключевую роль здесь играют Федеральная служба по техническому и экспортному контролю (ФСТЭК России), Федеральная служба безопасности (ФСБ России) и Роскомнадзор. ФСТЭК России осуществляет контроль за соблюдением требований

по защите информации, ФСБ России обеспечивает криптографическую и техническую защиту информации, а Роскомнадзор осуществляет контроль и надзор в сфере средств массовой информации и связи [9].

Уголовно-правовые механизмы защиты информационной безопасности представлены системой норм Уголовного кодекса РФ, устанавливающих ответственность за преступления в сфере компьютерной информации (глава 28 УК РФ), а также за иные преступления, связанные с информационной сферой. Данные механизмы направлены на предупреждение и пресечение наиболее общественно опасных деяний в информационной сфере, таких как неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных компьютерных программ, нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Гражданско-правовые механизмы защиты информационной безопасности включают в себя институты защиты интеллектуальной собственности, коммерческой тайны, персональных данных, а также общие способы защиты гражданских прав, предусмотренные статьей 12 Гражданского кодекса РФ. Данные механизмы позволяют правообладателям защищать свои права на информационные ресурсы и требовать возмещения убытков, причиненных нарушением их прав [6, с. 215].

Особое место в системе механизмов правовой защиты информационной безопасности занимают специализированные правовые режимы, такие как режим государственной тайны, режим коммерческой тайны, режим персональных данных, режим критической информационной инфраструктуры. Каждый из этих режимов предусматривает особый порядок создания, хранения, использования, распространения и защиты соответствующей информации, а также ответственность за нарушение установленных требований [3].

Эффективность механизмов правовой защиты информационной безопасности во многом зависит от их адаптивности к новым вызовам и угрозам в информационной сфере. Как отмечают Т.А. Полякова и Г.Г. Камалова, в условиях цифровой трансформации общества и государства особое значение приобретает развитие правовых механизмов защиты критической информационной инфраструктуры, противодействия компьютерным атакам и обеспечения информационного суверенитета государства [8, с. 119].

Анализ судебной и административной практики показывает, что наиболее эффективными являются комплексные механизмы правовой защиты, сочетающие превентивные, пресекательные и восстановительные меры. Так, в деле о нарушении требований законодательства о персональных данных одной из крупных интернет-компаний суд применил не только административный штраф, но и обязал компанию устранить выявленные нарушения и принять меры по предотвращению подобных нарушений в будущем [2, с. 36].

Важным элементом механизмов правовой защиты информационной безопасности является международное сотрудничество, которое реализуется через заключение международных договоров, участие в международных организациях и форумах по вопросам информационной безопасности, а также через механизмы правовой помощи по уголовным и гражданским делам. Как отмечает А.К. Дубень, эффективность противодействия трансграничным информационным угрозам напрямую зависит от уровня международного сотрудничества и гармонизации национальных законодательств в данной сфере [4, с. 255].

Таким образом, механизмы правовой защиты информационной безопасности представляют собой сложную многоуровневую систему, включающую в себя конституционно-правовые, административно-правовые, уголовно-правовые и гражданско-правовые средства и инструменты. Эффективность данной системы зависит от комплексного применения различных механизмов, их адаптивности к новым вызовам и угрозам, а также от уровня международного сотрудничества в

данной сфере. Дальнейшее совершенствование механизмов правовой защиты информационной безопасности должно осуществляться с учетом баланса интересов личности, общества и государства, а также с учетом международного опыта и лучших практик в данной области.

2.2 Проблемы правоприменительной практики в сфере информационной безопасности

Правоприменительная практика в сфере информационной безопасности сталкивается с рядом существенных проблем, обусловленных как несовершенством нормативно-правовой базы, так и сложностью самого объекта правового регулирования. Динамичное развитие информационных технологий создает ситуацию, когда правовое регулирование зачастую не успевает адаптироваться к новым вызовам и угрозам, что порождает правовые пробелы и коллизии. Анализ современной правоприменительной практики позволяет выявить ключевые проблемы, требующие системного решения для повышения эффективности правового обеспечения информационной безопасности.

Одной из центральных проблем является терминологическая неопределенность в законодательстве об информационной безопасности. Как отмечают Т.А. Полякова и Г.Г. Камалова, отсутствие единого легального определения понятия "информационная безопасность" в российском законодательстве создает трудности в правоприменительной практике, поскольку различные нормативные правовые акты могут по-разному интерпретировать данное понятие [8, с. 115]. Это приводит к неоднозначному толкованию правовых норм и, как следствие, к противоречивой правоприменительной практике. Кроме того, в законодательстве отсутствуют четкие определения таких понятий, как "информационная угроза", "информационный суверенитет", "информационная атака", что также затрудняет правоприменение.

Существенной проблемой является фрагментарность правового регулирования информационной безопасности. Нормы, регулирующие данную сферу, содержатся в различных нормативных правовых актах, относящихся к разным отраслям законодательства, что создает сложности в их системном применении. М.К. Водопьянова указывает на наличие противоречий между нормами информационного, административного и уголовного законодательства в части определения составов правонарушений в информационной сфере и мер ответственности за их совершение [2, с. 37]. Это приводит к ситуациям, когда одно и то же деяние может квалифицироваться по-разному в зависимости от субъективного усмотрения правоприменителя.

Проблема экстерриториальности информационных правонарушений также создает значительные трудности в правоприменительной практике. Трансграничный характер информационного пространства позволяет правонарушителям действовать с территории одного государства, нарушая законодательство другого, что затрудняет выявление, пресечение и расследование таких правонарушений. Как отмечает Э.В. Горян, отсутствие эффективных механизмов международного сотрудничества в сфере противодействия киберпреступности существенно снижает эффективность национальных правовых механизмов защиты информационной безопасности [3, с. 113]. Данная проблема усугубляется различиями в национальных законодательствах и отсутствием универсальных международных стандартов в данной сфере.

Серьезной проблемой является недостаточная эффективность механизмов защиты персональных данных. Несмотря на наличие специального законодательства в данной сфере, на практике возникают значительные трудности с обеспечением реальной защиты персональных данных граждан. Бакытбек Кызы Ай и Ж.И. Калбаев отмечают, что операторы персональных данных зачастую формально подходят к выполнению требований законодательства, ограничиваясь получением формального согласия субъекта на обработку его персональных

данных без обеспечения их реальной защиты [1, с. 38]. Это приводит к массовым утечкам персональных данных и нарушению прав граждан на неприкосновенность частной жизни.

Проблема обеспечения безопасности критической информационной инфраструктуры также требует особого внимания. Несмотря на принятие Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации", на практике возникают трудности с определением объектов критической информационной инфраструктуры и обеспечением их реальной защиты. Л.В. Магдилова указывает на недостаточную проработанность механизмов категорирования объектов критической информационной инфраструктуры и отсутствие четких критериев оценки их значимости [6, с. 217]. Это создает риски недостаточной защищенности наиболее важных информационных систем и сетей.

Существенной проблемой является также недостаточная квалификация правоприменителей в сфере информационной безопасности. Сложность и специфичность данной сферы требуют от судей, прокуроров, следователей и иных правоприменителей специальных знаний и навыков, которыми они зачастую не обладают. Ю.Н. Сосновская и Е.О. Бондарь отмечают, что отсутствие специализированных судебных составов по делам о правонарушениях в информационной сфере приводит к неоднородной судебной практике и затрудняет формирование единых подходов к разрешению данной категории дел [9]. Данная проблема усугубляется быстрым развитием информационных технологий, за которым правоприменители не всегда успевают следить.

Проблема доказывания в делах о правонарушениях в информационной сфере также представляет значительную сложность. Специфика электронных доказательств, их легкая изменяемость и уничтожаемость, а также отсутствие четких правовых механизмов их сбора, фиксации и оценки создают значительные трудности в правоприменительной практике. Д.М. Зуенко и Е.А. Осадчук

указывают на отсутствие единых стандартов работы с электронными доказательствами и недостаточную проработанность процессуальных аспектов их использования в судебном процессе [5, с. 480]. Это приводит к ситуациям, когда электронные доказательства признаются недопустимыми или недостоверными, что затрудняет привлечение виновных лиц к ответственности.

Недостаточная эффективность механизмов ответственности за нарушения в сфере информационной безопасности также является существенной проблемой. Е.А. Николаева и Ю.В. Тузовская отмечают, что существующие санкции зачастую не соответствуют степени общественной опасности правонарушений в информационной сфере и не оказывают должного превентивного воздействия [7]. Кроме того, сложность выявления и доказывания таких правонарушений приводит к высокой латентности и безнаказанности значительной части правонарушителей.

Для преодоления выявленных проблем правоприменительной практики в сфере информационной безопасности представляется необходимым реализовать комплекс мер, направленных на совершенствование законодательства и правоприменительной практики. В частности, целесообразно:

1. Разработать и законодательно закрепить единый понятийный аппарат в сфере информационной безопасности, включая легальные определения ключевых понятий.

2. Провести систематизацию законодательства об информационной безопасности, устранив существующие противоречия и пробелы.

3. Развивать международное сотрудничество в сфере противодействия киберпреступности, включая гармонизацию национальных законодательств и создание эффективных механизмов правовой помощи.

4. Совершенствовать механизмы защиты персональных данных, усилив ответственность операторов за нарушение требований законодательства и обеспечив реальную защиту прав субъектов персональных данных. 16

5. Детализировать механизмы обеспечения безопасности критической информационной инфраструктуры, разработав четкие критерии категорирования объектов и требования к их защите.

6. Повышать квалификацию правоприменителей в сфере информационной безопасности, включая создание специализированных судебных составов и подразделений правоохранительных органов.

7. Совершенствовать процессуальные механизмы работы с электронными доказательствами, разработав единые стандарты их сбора, фиксации и оценки.

8. Оптимизировать систему ответственности за правонарушения в информационной сфере, обеспечив соответствие санкций степени общественной опасности деяний и их превентивное воздействие.

Таким образом, правоприменительная практика в сфере информационной безопасности сталкивается с комплексом взаимосвязанных проблем, обусловленных как несовершенством нормативно-правовой базы, так и спецификой самого объекта правового регулирования. Решение данных проблем требует системного подхода, включающего совершенствование законодательства, развитие международного сотрудничества, повышение квалификации правоприменителей и оптимизацию механизмов ответственности. Только комплексный подход позволит повысить эффективность правового обеспечения информационной безопасности и обеспечить надежную защиту интересов личности, общества и государства в информационной сфере.

2.3 Совершенствование правового регулирования информационной безопасности

Динамичное развитие информационных технологий и постоянно эволюционирующий характер киберугроз обуславливают необходимость непрерывного совершенствования правового регулирования информационной безопасности. Анализ существующих проблем правоприменительной практики, а

также изучение международного опыта позволяют сформулировать ряд конкретных предложений по модернизации законодательства в данной сфере. Совершенствование правового регулирования должно осуществляться комплексно, затрагивая как концептуальные основы, так и конкретные правовые механизмы защиты информации.

Первостепенной задачей является унификация понятийного аппарата в сфере информационной безопасности. Целесообразно законодательно закрепить единое определение понятия "информационная безопасность" в базовом Федеральном законе "Об информации, информационных технологиях и о защите информации", а также разработать глоссарий основных терминов, используемых в данной сфере [3]. Это позволит устранить терминологические противоречия и создать единую концептуальную основу для правового регулирования. Как отмечают Т.А. Полякова и Г.Г. Камалова, унификация понятийного аппарата является необходимым условием эффективного правоприменения и формирования единообразной судебной практики [8, с. 117].

Важным направлением совершенствования правового регулирования является систематизация законодательства об информационной безопасности. Представляется целесообразным разработать и принять комплексный федеральный закон "Об информационной безопасности", который бы консолидировал основные положения, содержащиеся в различных нормативных правовых актах, и устранил существующие противоречия и пробелы. Данный закон должен определить основные принципы обеспечения информационной безопасности, полномочия государственных органов в данной сфере, права и обязанности субъектов информационных отношений, а также механизмы ответственности за нарушения в сфере информационной безопасности.

Совершенствование правового регулирования защиты персональных данных является одним из приоритетных направлений. Необходимо усилить ответственность операторов персональных данных за нарушение требований

законодательства, внедрить механизмы обязательного уведомления субъектов персональных данных о произошедших утечках, а также расширить полномочия уполномоченного органа по защите прав субъектов персональных данных [4]. Бакытбек Кызы Ай и Ж.И. Калбаев предлагают внедрить в российское законодательство элементы европейской модели защиты персональных данных, в частности, институт "права на забвение" и механизм обязательной оценки воздействия на защиту данных [1, с. 39].

Развитие правового регулирования безопасности критической информационной инфраструктуры требует детализации механизмов категорирования объектов и установления дифференцированных требований к их защите в зависимости от категории значимости. Целесообразно законодательно закрепить обязательность проведения регулярных аудитов безопасности объектов критической информационной инфраструктуры и установить четкие критерии оценки их защищенности [5]. Л.В. Магдилова предлагает внедрить риск-ориентированный подход к регулированию безопасности критической информационной инфраструктуры, при котором интенсивность контрольно-надзорных мероприятий будет зависеть от уровня риска, связанного с конкретным объектом [6, с. 218].

Совершенствование правового регулирования противодействия компьютерным преступлениям требует модернизации уголовного законодательства с учетом появления новых форм и методов совершения преступлений в информационной сфере. Необходимо расширить перечень составов преступлений в сфере компьютерной информации, включив в него такие деяния, как фишинг, кибервымогательство, кибертерроризм, а также дифференцировать ответственность в зависимости от тяжести последствий [9]. Е.А. Николаева и Ю.В. Тузовская предлагают также усилить уголовную ответственность за преступления против информационной безопасности несовершеннолетних [7].

Развитие международного сотрудничества в сфере информационной безопасности является необходимым условием эффективного противодействия трансграничным информационным угрозам. Целесообразно активизировать работу по заключению двусторонних и многосторонних соглашений о сотрудничестве в данной сфере, а также по гармонизации национального законодательства с международными стандартами [4, с. 256]. Особое внимание следует уделить развитию механизмов оперативного обмена информацией о киберугрозах и совместного расследования компьютерных преступлений.

Совершенствование процессуальных аспектов обеспечения информационной безопасности требует разработки специальных правил сбора, фиксации и оценки электронных доказательств, а также создания специализированных судебных составов по делам о правонарушениях в информационной сфере [2, с. 38]. Д.М. Зуенко и Е.А. Осадчук предлагают внедрить в процессуальное законодательство институт "электронного доказательства" с четким определением его признаков и порядка использования в судебном процессе [5, с. 481].

Таким образом, совершенствование правового регулирования информационной безопасности должно осуществляться комплексно, затрагивая различные аспекты данной сферы и учитывая как национальные интересы, так и международный опыт. Только системный подход, сочетающий унификацию понятийного аппарата, систематизацию законодательства, развитие специализированных правовых режимов, совершенствование механизмов ответственности и развитие международного сотрудничества, позволит создать эффективную правовую основу для обеспечения информационной безопасности в современных условиях.

ЗАКЛЮЧЕНИЕ

Проведенное исследование правового обеспечения информационной безопасности позволяет сформулировать ряд значимых выводов, имеющих как теоретическое, так и практическое значение. В современных условиях цифровой трансформации общества и государства вопросы правового обеспечения информационной безопасности приобретают особую актуальность и требуют комплексного подхода к их решению.

Анализ теоретико-правовых основ информационной безопасности показал, что данное понятие имеет многоаспектный характер и включает в себя защиту информации, информационных систем и информационной инфраструктуры от внешних и внутренних угроз, обеспечение конфиденциальности, целостности и доступности информации, а также защиту интересов личности, общества и государства в информационной сфере. Нормативно-правовое регулирование информационной безопасности в Российской Федерации представляет собой многоуровневую систему, включающую Конституцию РФ, федеральные законы, подзаконные акты и ведомственные нормативные документы.

Изучение международного опыта правового регулирования информационной безопасности выявило различные модели и подходы, обусловленные национальными особенностями и приоритетами. При этом наблюдается общая тенденция к усилению правового регулирования в ответ на растущие киберугрозы, развитию специализированного законодательства по защите критической информационной инфраструктуры и совершенствованию механизмов защиты персональных данных.

Исследование механизмов правовой защиты информационной безопасности показало, что наиболее эффективными являются комплексные механизмы, сочетающие конституционно-правовые, административно-правовые, уголовно-правовые и гражданско-правовые средства и инструменты. Однако

правоприменительная практика в данной сфере сталкивается с рядом проблем, включая терминологическую неопределенность, фрагментарность правового регулирования, экстерриториальность информационных правонарушений, недостаточную эффективность механизмов защиты персональных данных и безопасности критической информационной инфраструктуры.

Для совершенствования правового регулирования информационной безопасности необходимо реализовать комплекс мер, включающий унификацию понятийного аппарата, систематизацию законодательства, совершенствование правового регулирования защиты персональных данных и безопасности критической информационной инфраструктуры, модернизацию уголовного законодательства, развитие международного сотрудничества и механизмов государственно-частного партнерства.

Перспективными направлениями развития правового регулирования информационной безопасности являются внедрение риск-ориентированного подхода к регулированию, развитие правовых механизмов противодействия новым видам киберугроз, совершенствование процессуальных аспектов обеспечения информационной безопасности, а также гармонизация национального законодательства с международными стандартами.

Таким образом, эффективное правовое обеспечение информационной безопасности возможно только при комплексном подходе, учитывающем интересы личности, общества и государства, а также современные вызовы и угрозы в информационной сфере.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативно-правовые акты

1. Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 г. (в ред. от 25.03.2024) // Собрание законодательства Рос. Федерации. — 2024. — № 13. — Ст. 2023.

2. О безопасности : закон РФ от 5 марта 1992 г. № 2446-1 (в ред. от 04.03.2024) // Собрание законодательства Рос. Федерации. — 1992. — № 15. — Ст. 769.

3. Об информации, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 г. № 149-ФЗ (в ред. от 01.03.2024) // Собрание законодательства Рос. Федерации. — 2006. — № 31 (ч. I). — Ст. 3448.

4. О персональных данных : федер. закон от 27 июля 2006 г. № 152-ФЗ (в ред. от 01.04.2024) // Собрание законодательства Рос. Федерации. — 2006. — № 31 (ч. I). — Ст. 3451.

5. О безопасности критической информационной инфраструктуры Российской Федерации : федер. закон от 26 июля 2017 г. № 187-ФЗ (в ред. от 01.03.2024) // Собрание законодательства Рос. Федерации. — 2017. — № 31 (ч. I). — Ст. 4768.

Научная литература

6. Ай, Бакытбек Кызы, Калбаев Ж. И. Информационная безопасность в цифровой экономике: вопросы защиты данных в условиях растущих киберугроз // Вестник науки. — 2025. — № 1.3 (84). — С. 34–41.

7. Водопьянова, М. К. Конституционные гарантии приватности и киберугрозы: правовые коллизии защиты критической инфраструктуры // Вопросы российской юстиции. — 2025. — № 36. — С. 31–40.

8. Горян, Э. В. Информационная безопасность в киберпространстве: опыт правового регулирования Таиланда // Территория новых возможностей. Вестник Владивостокского государственного университета. — 2021. — Т. 13, № 3. — С. 108–116.

9. Дубень, А. К. Международный опыт правового регулирования информационной безопасности: правовые и информационные аспекты // Наукосфера. — 2022. — № 3-1. — С. 255.

10. Зуенко, Д. М., Осадчук Е. А. Конституционные аспекты обеспечения информационной безопасности и борьбы с киберугрозами в Российской Федерации // ББК 67.400 Редакционная коллегия. — 2023. — С. 477.

11. Магдилова, Л. В. Правовое регулирование сквозных технологий при обеспечении информационной безопасности государства // Москва. — 2023. — № 2. — С. 211–219.

12. Николаева, Е. А., Тузовская Ю. В. Гарантии информационных прав несовершеннолетних как способ защиты от киберугроз // Право и законность: вопросы теории и практики. — 2022.

13. Полякова, Т. А., Камалова Г. Г. Новые векторы развития системы правового обеспечения информационной безопасности как одного из приоритетов национальной безопасности (к 30-летию принятия закона Российской Федерации «О безопасности») // Правовое государство: теория и практика. — 2022. — № 2 (68). — С. 112–121.

14. Сосновская, Ю. Н., Бондарь Е. О. К вопросу об административно-правовом регулировании противодействия киберугрозам в современной России // Административно-правовое регулирование правоохранительной деятельности: теория и практика. — 2022.