

Министерство науки и высшего образования Российской Федерации
Ярославский государственный университет им. П. Г. Демидова
Кафедра социального и семейного законодательства

С. В. Симонова
Е. Н. Мазалецкая

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
В СОЦИАЛЬНОЙ И ЭКОНОМИЧЕСКОЙ СФЕРАХ

Учебно-методическое пособие

Ярославль
ЯрГУ
2023

УДК 349(075.8)
ББК Х623.3я73
С37

Рекомендовано
Редакционно-издательским советом университета
в качестве учебного издания. План 2023 года

Рецензенты:
Т. Р. Сурова, и. о. руководителя Управления
Роскомнадзора по Ярославской области,
кафедра социального и семейного законодательства
ЯрГУ им. П. Г. Демидова

Симонова, Снежана Владимировна.

С37 Правовое обеспечение информационной безопасности в социальной и экономической сферах : учебно-методическое пособие / С. В. Симонова, Е. Н. Мазалецкая ; Яросл. гос. ун-т им. П. Г. Демидова. — Ярославль : ЯрГУ, 2023. — 44 с.

Пособие содержит рекомендации к изучению тем курса, списки основных литературных и нормативно-правовых источников, материалы судебной практики.

Предназначено для студентов, изучающих дисциплину «Правовое обеспечение информационной безопасности в социальной и экономической сферах».

УДК 349(075.8)
ББК Х623.3я73

© ЯрГУ, 2023

О курсе «Правовое обеспечение информационной безопасности в социальной и экономической сферах»

Курс «Правовое обеспечение информационной безопасности в социальной и экономической сферах» был разработан в 2021–2022 гг. в рамках проекта, реализуемого победителем конкурса на предоставление грантов преподавателям магистратуры благотворительной программы «Стипендиальная программа Владимира Потанина» Благотворительного фонда Владимира Потанина.

Актуальность курса особенно ярко подчеркивается на фоне тенденции ежегодного увеличения количества и многообразия угроз информационной безопасности граждан, бизнеса и объектов социальной сферы, роста числа и результативности кибератак. Возрастает востребованность специалистов, умеющих выявлять и юридически нивелировать риски информационной безопасности, организовать режим правовой защиты различных видов данных компаний и граждан.

Курс позволит получить знания, умения и навыки, необходимые для системной работы с информацией и данными в бизнесе и государственном секторе. Вы овладеете нюансами юридического сопровождения оборота информации и обеспечения её конфиденциальности, компетенциями по защите прав и интересов в информационной сфере.

Изучение и закрепление материала будет проходить на примере реальных кейсов компаний-партнеров проекта, с учетом материалов самой актуальной нормативной и правоприменительной практики, что делает курс максимально практикоориентированным и отвечающим потребностям реального сектора экономики. Занятия курса будут проходить в форме видеолекций, подкастов, кейс-сессий и вебинаров, что делает процесс обучения максимально современным и интересным.

В состав команды разработчиков программы курса вошли С. В. Симонова, канд. юрид. наук, доцент кафедры социального и семейного законодательства ЯрГУ им. П. Г. Демидова, Е. Н. Мазалецкая, директор Центра поддержки технологий и инноваций ЯрГУ им. П. Г. Демидова, Т. Р. Сурова, исполняющий обязанности руководителя Управления Роскомнадзора по Ярославской области. Неоценимый вклад в разработку кейсов и материалов практических занятий курса внесли партнеры проекта — Управление Роскомнадзора по Ярославской области, компании «Тензор», «Лаборатория мультимедиа», «Стандарт безопасности», «DrCash», НПО «Криста», «Компания инновационного бизнеса», «Инсти-

тут защиты данных», «Информационные технологии», которым мы выражаем искреннюю признательность за сотрудничество.

В качестве **основных** рекомендуются следующие **источники**.

Литературные (учебные издания)

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / под ред. Т. А. Поляковой, А. А. Стрельцова. — Москва : Юрайт, 2021. — 325 с. — URL : <https://urait.ru/viewer/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-469235#page/2>

2. Архипов, В. В. Интернет-право : учебник и практикум для вузов. / В. В. Архипов. — М.: Юрайт, 2020. — 249 с. — URL : <https://www.biblio-online.ru/viewer/internet-pravo-450761#page/1>

3. Волков, Ю. В. Информационное право. Информация как правовая категория : учеб. пособие для вузов / Ю. В. Волков. — Москва : Юрайт, 2020. — 109 с. — URL : <https://www.biblio-online.ru/viewer/informacionnoe-pravo-informaciya-kak-pravovaya-kategoriya-455553#page/2>

4. Информационное право : учебник для вузов / М. А. Федотов и др. — Москва : Юрайт, 2020. — 497 с. — URL : <https://www.biblio-online.ru/viewer/informacionnoe-pravo-451031#page/2>

5. Бачило, И. Л. Информационное право: учебник для вузов / И. Л. Бачило. — Москва : Юрайт, 2020. — 419 с. — URL : <https://www.biblio-online.ru/viewer/informacionnoe-pravo-449666#page/2>

6. Рассолов, И. М. Информационное право: учебник и практикум для вузов / И. М. Рассолов. — Москва : Юрайт, 2020. — 347 с. — URL : <https://www.biblio-online.ru/viewer/informacionnoe-pravo-449839#page/2>

7. Цифровое право : учебник / под общ. ред. В. В. Блажеева, М. А. Егоровой. — Москва : Проспект, 2020. — 640 с. — URL : <http://ebs.prospekt.org/book/42840/page/1>

Нормативно-правовые источники

Конституция РФ.

Гражданский кодекс РФ (части 1–4).

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. — 2006. — № 31 (1 ч.), ст. 3448.

Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности» // СЗ РФ. — 2011. — № 1, ст. 2.

Федеральный закон от 31.07.2020 № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» // СЗ РФ. — 2020. — № 31 (Часть I), ст. 5007.

Указ Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» // СЗ РФ. — 2008. — № 12, ст. 1110.

Указ Президента РФ от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации» // СЗ РФ. — 2015. — № 21, ст. 3092.

Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. — 2016. — № 50, ст. 7074.

Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» // СПС «КонсультантПлюс».

Национальные стандарты в области информационной безопасности

Информационная безопасность. Документы. — URL : <https://www.msu.ru/info/is/docs/gosstand.pdf>

Информационные ресурсы

Научная библиотека ЯрГУ. — URL : <http://www.lib.uniyar.ac.ru>

Электронная библиотечная система «Университетская библиотека Online». — URL : www.biblioclub.ru

Научная электронная библиотека «eLIBRARY.ru». — URL : <http://elibrary.ru>

Официальный интернет-портал правовой информации. — URL : <http://pravo.gov.ru/>

Судебные и нормативные акты РФ. — URL : <http://sudact.ru/>

Президент РФ. — URL : <http://www.kremlin.ru>

Правительство РФ. — URL : <http://government.ru>

Министерство цифрового развития, связи и массовых коммуникаций РФ. — URL : <https://digital.gov.ru/ru/>

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. — URL : <https://rkn.gov.ru>

ФСБ России. — URL : <http://www.fsb.ru>

ФСТЭК России. — URL : <https://fstec.ru>

Федеральная служба по интеллектуальной собственности. — URL : <https://rospatent.gov.ru/ru>

Федеральный институт промышленной собственности. — URL : <https://www1.fips.ru>

Всемирная организация по интеллектуальной собственности. — URL : <https://www.wipo.int/portal/en/index.html>

Ярославская Областная дума. — URL : <http://yarduma.ru/>

Конституционный суд РФ. — URL : <http://www.ksrf.ru/ru/>

Верховный суд РФ. — URL : <http://vs.pf>

Федеральные арбитражные суды РФ. — URL : <http://www.arbitr.ru>

ФАС Волго-Вятского округа. — URL : <https://fasvvo.arbitr.ru>

Второй арбитражный апелляционный суд. — URL : <http://2aas.arbitr.ru>

Арбитражный суд Ярославской области. — URL : <https://yaroslavl.arbitr.ru>

Ярославский областной суд. — URL : <http://oblsud.jrs.sudrf.ru>

Тема 1. Понятие и правовые основы информационной безопасности в социальной и экономической сферах

1. Информация как объект социально-экономических отношений.
2. Основные виды информационных угроз в социальной и экономической сферах и юридические механизмы их нейтрализации.
3. Понятие, юридические средства и система мер обеспечения информационной безопасности в социальной и экономической сферах.
4. Национально-правовые и международные основы обеспечения информационной безопасности в социальной и экономической сферах.
5. Основания и порядок ограничения доступа к информации.
6. Ответственность за нарушения в сфере оборота информации при реализации социальных и экономических прав.

Рекомендуемые дополнительные источники

Литературные

1. Гродзенский, Я. С. Информационная безопасность : учеб. пособие / Я. С. Гродзенский. — Москва : РГ-Пресс, 2020. — 144 с. — URL : <http://ebs.prospekt.org/book/43070>
2. Симонова, С. В. Административно-процессуальные аспекты реализации запретов распространения информации в сети «Интернет» // Вестник Ярославского государственного университета им. П. Г. Демидова. Серия : Гуманитарные науки. — 2021. — № 4. — С. 84–91. — URL : https://elibrary.ru/download/elibrary_44805896_13279092.pdf
3. Юрченко, И. А. Преступления против информационной безопасности : учеб. пособие / И. А. Юрченко. — Москва : Проспект, 2021. — 208 с. — URL : <http://ebs.prospekt.org/book/44295>

Нормативно-правовые

1. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании» // СЗ РФ. — 2002. — № 52 (Часть I), ст. 5140.
2. Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» // СЗ РФ. — 2011. — № 19, ст. 2716.
3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СЗ РФ. — 2017. — № 31 (Часть I), ст. 4736.

4. Постановление Правительства РФ от 03.03.2012 № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации» // СЗ РФ. — 2012. — № 11, ст. 1297.

5. Приказ ФСБ РФ № 416, ФСТЭК РФ № 489 от 31.08.2010 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования» // Российская газета. — 2010. — 22 окт.

Методические и руководящие документы

1. Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. Гостехкомиссией РФ 25.11.1994) // СПС «КонсультантПлюс».

2. Методический документ. Методика оценки угроз безопасности информации (утв. ФСТЭК России 05.02.2021) // СПС «КонсультантПлюс».

3. Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014) // СПС «КонсультантПлюс».

Информационные материалы

1. Угрозы информационной безопасности. SEARCHINFORM. — URL : <https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti/>

2. Основы информационной безопасности // SEARCHINFORM. — URL : <https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/>

Введение в тему

Под информационной безопасностью понимается такое состояние элементов информационной сферы, при которых они наименее восприимчивы к вмешательству (незаконному доступу, изучению, использованию), нанесению ущерба (уничтожению), разглашению со стороны третьих лиц. В целом режим безопасности предполагает управление рисками, связанными с разглашением информации или влиянием на аппаратные и программные модули защиты. К числу элементов информационной сферы относятся информация (сведения, сообщения, данные); базы данных; объекты информационной инфраструктуры (объекты информатизации, информационные системы, сайты, сети связи); а также субъекты информационной сферы.

Информация является базисом информационной сферы и определяется в действующем законодательстве через призму принимающих любую

форму сведений. Обращает на себя внимание, что законодатель ставит условный знак равенства между такими категориями, как «информация», «сообщения» и «данные», хотя в теории информационной и компьютерной безопасности эти понятия разграничиваются.

Базовая классификация различных видов информации в настоящее время представлена в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Федеральный закон № 149-ФЗ). В соответствии с этим нормативным правовым актом в зависимости от категории доступа выделяются *общедоступная информация* (общеизвестная и другая информация, доступ к которой не ограничен) и *информация ограниченного доступа* (различные виды тайн — банковская, врачебная, тайна связи, нотариальная тайна и пр.). Опираясь на критерий порядка распространения и предоставления информации, можно выделить *свободно распространяемую информацию*; *информацию, предоставляемую по соглашению лиц, участвующих в отношениях*; *информацию, которая подлежит распространению или предоставлению в соответствии с федеральным законом*; *информацию, распространение которой ограничивается или запрещается*.

В качестве субъектов информационной сферы особо выделяются обладатели информации или субъекты, обладающие правомочиями владеть, пользоваться и распоряжаться составляющими информационной инфраструктуры; субъекты обеспечения безопасности информации и информационной инфраструктуры; пользователи информации или субъекты информации (например, субъекты персональных данных).

Комплексное определение понятия информационной безопасности РФ приводится в утвержденной Указом Президента РФ от 05.12.2006 № 646 «Доктрине информационной безопасности» как состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Режим информационной безопасности отличают следующие основные характеристики: 1) его функциональная направленность, обеспечивающая связь с конкретным объектом, защита которого обеспечивается; 2) определение объектов защиты на уровне руководителей организации, должностных лиц, законодателя; 3) отнесение объектов защиты к числу объектов информационной сферы.

Угрозы информационной безопасности можно определить как вероятные или реальные попытки посягательства на объекты информационной сферы, полноту, целостность и доступность данных. В самом общем виде справедливо утверждать, что угрозы указывают на наличие уязвимых, «слабых» мест в целостной системе данных. Целостность данных предполагает сохранение постоянной структуры и содержания информации при её передаче и хранении. Свойство достоверности данных выражается в их подтверждении определенными субъектами. Наконец, доступ к информации предполагает возможность её копирования, обработки и удаления по усмотрению субъекта.

К основным способам получения доступа относятся *несанкционированный доступ* (незаконное использование данных), *утечка* (неконтролируемое распространение информации за пределы сети) и разглашение, выступающее следствием человеческого фактора. Несанкционированный доступ может осуществляться как посредством воздействия на субъектов информационной сферы, так и с помощью программного обеспечения или аппаратных компонентов автоматизированной системы.

В зависимости от источника возникновения подобные угрозы могут иметь *внутренний* или *внешний*, *объективный* или *субъективный характер*. Внешние угрозы информационной безопасности могут сопровождаться взломом аккаунтов, сетей, серверов и пр., тогда как внутренние угрозы связаны с неправомерными действиями сотрудников и органов управления компании.

К числу основных уровней защиты информации относятся мероприятия *законодательного уровня*, *административного уровня*, *мероприятия по защите информации*, *практические мероприятия*.

Говоря об информационной безопасности компаний, стоит упомянуть, что создание системы защиты информации осуществляется в несколько этапов. На первом производится разработка базовой модели системы защиты, определяются система конфиденциальной информации и подлежащие защите источники информации, выявляются цели получения доступа к защищаемой информации и способы такового. На втором этапе производится разработка системы защиты на нескольких уровнях — правовом, организационном и техническом. Организационный уровень предполагает разработку регламентов работы с конфиденциальной информацией, кадровую работу, организацию работы с документацией и физическими носителями данных. Технический уровень предполагает создание преград вокруг защищаемого объекта, установку технических средств, программные и математические средства. Наконец, на третьем

этапе производится поддержка работоспособности системы, её регулярный контроль и управление рисками.

Одной из целей, для достижения которой в государстве вводится правовое регулирование защиты информации, служит цель обеспечения прав и свобод человека в информационной сфере. К числу таковых прав относятся право на информацию, права на объекты интеллектуальной собственности, свобода массовой информации. Немаловажно и то, что правовой режим информационной безопасности обеспечивает защиту различного рода «тайн» и иной конфиденциальной информации — персональных данных, коммерческой тайны, служебной тайны и пр. Наконец, правовое регулирование отношений в области информационной безопасности обеспечивает защиту информационных и телекоммуникационных технологий и объектов информационной инфраструктуры (электронной подписи, информационных систем, интернет-технологий, средств обеспечения информационной безопасности).

Систему актов, составляющих правовые основы информационной безопасности, возглавляют Конституция РФ и международные правовые акты, гарантирующие права человека в информационной сфере. Важно обратить внимание на то, что в силу прямого указания положений п. «м» ст. 71 Конституции РФ обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных относятся к ведению Российской Федерации.

Основным федеральным нормативным правовым актом, регулирующим отношения в информационной сфере, в настоящее время является Федеральный закон № 149-ФЗ, положения которого развиваются в других актах, обеспечивающих безопасность отдельных видов информации, объектов информационных инфраструктуры и информационных технологий (например, закон РФ от 21.07.1993 № 5485-1 «О государственной тайне», Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи», иные правовые акты).

Кроме того, в системе правовых основ обеспечения информационной безопасности особо выделяются нормативно-технические акты — подзаконные акты, технические и административные внутренние регламенты, инструкции, стандарты (например, акты ФСТЭК России, ФСБ России и др.).

Вопросы для дискуссии

1. Каково соотношение понятий «информационная безопасность», «кибербезопасность», «сетевая безопасность» и «компьютерная безопасность»?

2. Как может быть определено место права информационной безопасности в системе российского права?

3. В каких изменениях и дополнениях нуждаются положения Федерального закона «Об информации, информационных технологиях и о защите информации» в целях повышения уровня защищенности прав и интересов граждан в информационной сфере?

Задания

1. Ознакомившись с видеолекцией С. В. Симоновой «Базовые понятия права информационной безопасности», дайте определение информационной безопасности.

2. Опираясь на положения «Доктрины информационной безопасности РФ» 2016 г., вставьте недостающие слова в определение:

«Информационная инфраструктура РФ — это совокупность объектов _____, информационных _____, сайтов в сети _____ и сетей _____, расположенных на территории РФ, а также на территориях, находящихся под юрисдикцией РФ или используемых на основании международных договоров РФ».

3. Ознакомьтесь с видеолекцией С. В. Симоновой «Правовые основы информационной безопасности» и приведите по одному примеру следующих типов информационных сведений:

- свободно распространяемая информация;
- информация, предоставляемая по соглашению лиц;
- информация, подлежащая предоставлению в соответствии с федеральным законом;
- информация, распространение которой запрещается;
- информация, распространение которой ограничивается.

4. Ознакомившись со ст. 15.1 Федерального закона «Об информации, информационных технологиях и о защите информации», сформулируйте пошаговый алгоритм ограничения доступа к запрещенной информации в сети «Интернет».

5. Ознакомьтесь с видеолекцией Д. М. Мурина «Правовые основы обеспечения информационной безопасности. Введение» по ссылке <https://www.youtube.com/watch?v=YHRfZz3OD3c&list=PLPwVWatt1r8->

O0yO6ibxiE4YyGhdNJIQq&index=2&t=28s и укажите два подхода к защите информации, о которых ведет речь лектор.

6. Ознакомьтесь с видеолекцией Д. М. Мурина «Правовые основы обеспечения информационной безопасности. Информация и ее характеристика» по ссылке <https://www.youtube.com/watch?v=TS3SNt-1e9c&list=PLPwVWatt1r8-O0yO6ibxiE4YyGhdNJIQq&index=3> и укажите основные характеристики (свойства) безопасности информации, о которых ведет речь лектор.

7. Ознакомьтесь с видеолекцией Д. М. Мурина «Правовые основы обеспечения информационной безопасности. Классификация информации с точки зрения возможности распространения» по ссылке https://www.youtube.com/watch?v=Nv4Xf2or_mw&list=PLPwVWatt1r8-O0yO6ibxiE4YyGhdNJIQq&index=5 и зафиксируйте два формата передачи информации, о которых рассказывает лектор.

8. Ознакомьтесь с видеолекцией Д. М. Мурина «Правовые основы обеспечения информационной безопасности. Информационные системы» по ссылке https://www.youtube.com/watch?v=sfsy_G3l4MU&list=PLPwVWatt1r8-O0yO6ibxiE4YyGhdNJIQq&index=6 и укажите два основных объекта защиты, о которых ведет речь лектор.

Тема 2. Режим конфиденциальности информации

1. Понятие и особенности режима конфиденциальности информации.
2. Виды конфиденциальных сведений.
3. Правовой режим коммерческой тайны.
4. Защита служебной и профессиональной тайны.
5. Правовой режим банковской тайны и тайны страхования.
6. Право на секрет производства (ноу-хау).
7. Правовая охрана тайны усыновления.

Рекомендуемые дополнительные источники

Литературные

1. Илякова, И. Е. Коммерческая тайна : учеб. пособие для вузов / И. Е. Илякова. — Москва : Юрайт, 2022. — 139 с. — URL : <https://urait.ru/book/kommercheskaya-tayna-497149>

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под ред. Т. А. Поляковой,

А. А. Стрельцова. — Москва : Юрайт, 2022. — 325 с. — URL : <https://urait.ru/bcode/498844>

3. Шерстобитов, А. Е. Секрет производства («ноу-хау») : понятие, охраноспособность, осуществление исключительного права / А. Е. Шерстобитов // Законы России : опыт, анализ, практика. — 2019. — № 9. — С. 34–38. — URL : <https://elibrary.ru/item.asp?id=41025832>

Нормативно-правовые

1. Трудовой кодекс РФ от 30.12.2001 № 197-ФЗ.
2. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ.
3. Уголовный кодекс РФ от 13.06.1996 № 63-ФЗ.
4. Семейный кодекс РФ от 29.12.1995 № 223-ФЗ.
5. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // СЗ РФ. — 2004. — № 32, ст. 3283.
6. Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» // СЗ РФ. — 1996. — № 6, ст. 492.
7. Указ Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» // СЗ РФ. — 1997. — № 10, ст. 1127.

Юридическая практика

1. Постановление Конституционного Суда РФ от 16.06.2015 № 15-П «По делу о проверке конституционности положений статьи 139 Семейного кодекса Российской Федерации и статьи 47 Федерального закона "Об актах гражданского состояния" в связи с жалобой граждан Г. Ф. Грубич и Т. Г. Гущиной» // СЗ РФ. — 2015. — № 26, ст. 3944.
2. Постановление Конституционного Суда РФ от 14.05.2003 № 8-П «По делу о проверке конституционности пункта 2 статьи 14 Федерального закона "О судебных приставах" в связи с запросом Лангепасского городского суда Ханты-Мансийского автономного округа» // СЗ РФ. — 2003. — № 21, ст. 2058.

Введение в тему

Конфиденциальность информации определяется в Федеральном законе № 149-ФЗ как обязательное для выполнения лицом, получившим доступ к определенной информации, требования не передавать такую информацию третьим лицам без согласия её обладателя. В самом общем виде правовой режим конфиденциальности информации включает в себя

ограниченный доступ к информации (устанавливается законом или договором), запрет на передачу информации без согласия её обладателя; запрет на распространение информации любым способом.

Перечень сведений конфиденциального характера в России установлен на уровне Указа Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера». К числу таковых относятся персональные данные, профессиональная тайна, служебная тайна, коммерческая тайна и иные виды охраняемой законом тайны, информация, в отношении которой режим конфиденциальности установлен договором, а также ряд иных конфиденциальных сведений.

Механизмы введения режима конфиденциальности в отношениях контрагентов достаточно разнообразны. В числе основных можно отметить такие способы, как, например, заключение отдельного письменного соглашения о конфиденциальности (NDA), относящегося к непоименованным в Гражданском кодексе РФ договорам; включение условия о конфиденциальности в договор между контрагентами; заключение дополнительного к уже заключенному договору соглашения о конфиденциальности. Одним из важных условий такого соглашения служит условие о его предмете, определяющем перечень конфиденциальных сведений, а также обязанность контрагента по сохранению их конфиденциальности. Указанное соглашение должно предусматривать и порядок передачи и использования конфиденциальной информации (например, порядок фиксации факта передачи данных, уполномоченное на соответствующие действия лицо, порядок использования переданной информации). Немаловажно определить и меры защиты информации (особые правила хранения носителя информации, фиксация движения информации, недопущение копирования информации), а также санкции за разглашение конфиденциальных сведений.

Одним из особых видов конфиденциальной информации является коммерческая тайна, определяемая в законодательстве через призму режима конфиденциальности информации, позволяющего её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ услуг или получить иную коммерческую выгоду. Информацию, составляющую коммерческую тайну, отличает её действительная или потенциальная коммерческая ценность, которая основывается на обстоятельстве неизвестности этой информации третьим лицам. Особенно коммерческой тайны служит и то, что у третьих лиц отсутствует свободный доступ к коммерческой тайне на законном основании. Важно,

что обладатель коммерческой тайны должен принимать меры по обеспечению её секретности (конфиденциальности). Соответствующие меры образуют режим коммерческой тайны.

В Федеральном законе от 29.07.2004 № 98-ФЗ «О коммерческой тайне» отсутствует перечень информации, которая может быть определена в качестве таковой. Напротив, приводится закрытый список сведений, которые не могут быть отнесены к коммерческой тайне. В их числе сведения, содержащиеся в учредительных документах юридического лица; сведения о численности, составе работников, о системе оплаты труда, о наличии свободных рабочих мест, об условиях и охране труда, о задолженности работодателя по заработной плате и социальным выплатам, а также ряд иных сведений.

Любая информация за рамками этого списка, отвечающая критериям коммерческой тайны, может быть определена в качестве таковой. К примеру, перечень сведений, составляющих коммерческую тайну, может включать логины и пароли для доступа к информации в электронном виде, информацию о системе ценообразования и ходе переговоров с покупателями, сведения о взаимодействии структурных подразделений, о контрагентах, об объеме товарооборота с клиентами.

Механизм введения режима коммерческой тайны в компании включает в себя следующую последовательность действий:

- определение перечня информации, составляющей коммерческую тайну;
- установление порядка обращения с этой информацией и обеспечение контроля его соблюдения;
- учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым она передана или предоставлена;
- урегулирование отношений по использованию информации, составляющей коммерческую тайну, с сотрудниками и контрагентами;
- нанесение грифа «коммерческая тайна» на материальные носители с секретной информацией.

Вопросы для дискуссии

1. Как соотносятся понятия коммерческой тайны и конфиденциальной информации?
2. Какие сведения составляют коммерческую тайну?
3. Существуют ли такие сведения, которые не могут быть отнесены к коммерческой тайне?

4. Могут ли быть отнесены к коммерческой тайне персональные данные? Сведения о заработной плате сотрудников?
5. Какие сведения относятся к служебной тайне?
6. В каком порядке может быть установлен режим коммерческой тайны?
7. Насколько обязательным является утверждение положения о коммерческой тайне в организациях?
8. Какие меры важно предпринять в организации в целях предотвращения разглашения коммерческой тайны сотрудниками?
9. Каким образом можно предотвратить разглашение конфиденциальной информации контрагентами?
10. Что такое NDA? В каком порядке может быть заключено данное соглашение и что важно учесть при его составлении?
11. Что считается разглашением конфиденциальной информации?
12. Какая ответственность наступает за разглашение коммерческой тайны?

Задания

Ознакомьтесь с видеолекцией С. В. Симоновой «Режим конфиденциальности информации» и выполните следующие задания.

1. Дайте понятие конфиденциальности информации и приведите примеры (не менее трех) сведений конфиденциального характера.
2. Укажите, что представляет собой NDA и какие положения (правила) должны быть закреплены в этом документе?
3. Опишите механизм введения режима конфиденциальности сведений в отношениях контрагентов.

Ознакомьтесь с видеолекцией С. В. Симоновой «Правовой режим коммерческой тайны» и выполните следующие задания.

4. Вставьте недостающие слова в определение коммерческой тайны:
«Коммерческая тайна — режим _____ информации, позволяющий её обладателю при существующих или возможных обстоятельствах _____ доходы, избежать неоправданных _____, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую _____».
5. Укажите, как соотносятся понятия «коммерческая тайна» и «ноу-хау».
6. Приведите примеры (не менее пяти) сведений, которые **не могут** составлять коммерческую тайну.

7. Приведите примеры (не менее пяти) сведений, которые **могут** составлять коммерческую тайну.

8. Опишите процедуру введения и обеспечения в организации режима коммерческой тайны.

9. Установите, какие обязанности налагаются в целях охраны коммерческой тайны:

а) на обладателя информации, составляющей коммерческую тайну; руководителя организации;

б) работодателя;

в) работников.

10. Определите, какие виды и меры ответственности установлены за нарушение режима коммерческой тайны.

Задачи

1. К вам обратился за юридической консультацией владелец агентства по запуску онлайн-продуктов с запросом о разработке юридического механизма, предотвращающего разглашение конфиденциальной информации клиентов агентства (авторов онлайн-курсов) со стороны членов команды. Руководитель агентства имеет статус самозанятого, все члены команды, с кем он сотрудничает, официально не трудоустроены, привлекаются для выполнения отдельных видов технических работ без подписания договоров (поддержка вебинаров, работы по дизайну, настройка «GetCourse» и пр.). Команда интернациональная: в нее входят фрилансеры из России, Украины и Беларуси. При этом каждый из них в той или иной мере получает доступ к логину и паролю от личного кабинета автора курса на образовательной платформе, к базе слушателей курса, владеет информацией о числе слушателей курсов и оборотах онлайн-школ. Логины и пароли скидываются клиентами агентства в закрытый чат в Telegram, куда включены руководитель агентства и члены его команды.

Оцените ситуацию и дайте развернутую юридическую консультацию владельцу агентства по его запросу.

2. IT-компания «N» ведет фактическую деятельность в следующих юрисдикциях: Россия, Ирландия, Англия и ОАЭ, в каждой из которых имеется зарегистрированное юридическое лицо. Большая часть команды (70 %) компании устроены в России, откуда и ведется непосредственно вся деятельность. При этом сотрудничество с контрагентами и клиентами ведется от имени юридических лиц из зарубежных юрисдикций. Перед тем как приступить к работе, каждый сотрудник компании дает обязательство о нераз-

глашении конфиденциальной информации, подписывая NDA с российским юридическим лицом. Форма NDA разработана на основе действующего в российском юридическом лице Положения о коммерческой тайне. Компания поставила перед юристами следующие вопросы:

1. Каким образом ей организовать свою структуру и взаимодействие между компаниями в разных юрисдикциях так, чтобы максимально защитить конфиденциальную информацию всех трех юридических лиц (клиентскую базу, персональные данные клиентов, коммерческую тайну) от действий недобросовестных сотрудников и конкурентов?

2. Какова юридическая сила подписываемых членами команды NDA и на что можно рассчитывать в случае его нарушения? Каковы перспективы привлечения к ответственности лиц, нарушивших принятые на себя посредством NDA обязательства?

Тема 3. Правовое обеспечение безопасности персональных данных

1. Понятие и виды персональных данных.
2. Принципы обработки персональных данных.
3. Документы оператора персональных данных.
4. Правовые основы государственного контроля (надзора) за обработкой персональных данных.
5. Политика в отношении обработки персональных данных: понятие и основные требования.

Рекомендуемые **дополнительные источники**

Литературные

1. Михайлова, И. А. Персональные данные и их правовая охрана : некоторые проблемы теории и практики / И. А. Михайлова // Законы России : опыт, анализ, практика. — 2017. — № 10. — С. 11–18. — URL : <https://elibrary.ru/item.asp?id=30575445>

2. Платонова, Н. И. Современный подход к пониманию персональных данных / Н. И. Платонова // Право и современные государства. — 2017. — № 5. — URL : <https://elibrary.ru/item.asp?id=32278669>

3. Савельев, А. И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных» / А. И. Савельев. — Москва : Статут, 2017. — URL : <https://elibrary.ru/item.asp?id=30659635>

Нормативно-правовые

1. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (заключена в г. Страсбурге 28.01.1981) // Бюллетень международных договоров. — 2014. — № 4.

2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. — 2006. — № 31 (1 ч.), ст. 3451.

3. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // СЗ РФ. — 2008. — № 38, ст. 4320.

4. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // СЗ РФ. — 2012. — № 45, ст. 6257.

5. Постановление Правительства РФ от 29.06.2021 № 1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных» // СЗ РФ. — 2021. — № 27 (ч. III), ст. 5424.

6. Приказ Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» // Российская газета. — 2013. — 18 сент.

Методические и руководящие документы

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК РФ 15.02.2008) // СПС «КонсультантПлюс».

Юридическая практика

Постановление Конституционного Суда РФ от 25.05.2021 № 22-П «По делу о проверке конституционности пункта 8 части 1 статьи 6 Федерального закона "О персональных данных" в связи с жалобой общества с ограниченной ответственностью "МедРейтинг"» // СЗ РФ. — 2021. — № 22, ст. 3915.

Введение в тему

Термин «персональные данные» непосредственно связан с частной жизнью человека и появился в российском законодательстве в середине 1990-х гг. Положениями Федерального закона от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации» (ныне утратил силу) персональные данные были отнесены к категории конфиденциаль-

ной информации, был установлен запрет на сбор, хранение, использование и распространение информации о частной жизни. При этом содержание понятия «персональные данные» на тот момент не раскрывалось.

Лишь в 1997 г. появляется некая конкретика относительно содержания понятия персональных данных. 6 марта 1997 г. был издан указ президента РФ, утвердивший перечень сведений конфиденциального характера. Согласно этому документу персональные данные «включают в себя сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность».

Современное законодательство Российской Федерации в области персональных данных основано на международных договорах Российской Федерации, Конституции РФ, федеральных законах и иных нормативных правовых актах РФ, а также законах и иных нормативных актах субъектов Российской Федерации. Основным документом, устанавливающим фундаментальные положения защиты персональных данных, является Федеральный закон от 27.07.2006 152-ФЗ «О персональных данных» (далее — Закон о персональных данных), который преследует цель обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных. Указанным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой юридическими и физическими лицами, государственными и муниципальными органами власти как с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, так и без использования таких средств.

В Законе о персональных данных персональные данные определяются в качестве любой информации, прямо или косвенно относящейся к субъекту персональных данных — определенному или определяемому физическому лицу. Обращает на себя внимание то, что соответствующая дефиниция основана на терминологии Европейской конвенции по защите персональных данных, ратифицированной Россией в 2005 г.

Как следует из определения персональных данных, закрытого перечня соответствующих сведений нет. При этом основным критерием, используемым для определения сведений в качестве персональных данных, служит «относимость» соответствующей информации к конкретному лицу и возможность идентификации последнего.

Из логики действующего Закона о персональных данных вытекает условное деление персональных данных на отдельные виды. «Общие» персональные данные включают в себя любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому

лицу (субъекту персональных данных), например фамилия, имя, отчество, адрес, электронная почта, дата рождения и др. (п. 1 ст. 3 Закона о персональных данных). К специальным категориям персональных данных относится информация, касающаяся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни физического лица (ч. 1 ст. 10 Закона о персональных данных). В особую группу выделяются биометрические персональные данные — сведения, характеризующие его физиологические особенности (сетчатка глаза, голос, отпечатки пальцев), которые позволяют установить его личность и используются оператором для установления личности субъекта (ст. 11 Закона о персональных данных).

Кроме того, в условиях цифровизации нельзя не выделить еще один вид персональных данных, который создается автоматически в цифровой среде: это электронные письма, регистрационные данные на сайтах социальных сетей, геопозиция физического лица. Персональные данные в цифровой среде можно также разграничить на так называемые «содержательные данные» и метаданные — «данные о данных». К содержательным данным, создаваемым человеком или устройствами, относятся текстовые, видео- и фотосообщения, разговоры, передаваемые через интернет-файлы. Метаданные создаются только электронными приборами: cookie-файлы в браузере, журналы входящих/исходящих звонков, геопозиционные метки в фотографиях при съемке, видео-, аудиомониторинге и т.п.

В соответствии с положениями ст. 3 Закона «О персональных данных» обработка персональных данных представляет собой любое действие (операцию) или совокупность действий (операций), совершаемых с использованием или без использования средств автоматизации, с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных. При этом при обработке персональных данных необходимо руководствоваться рядом принципов.

В числе основных принципов обработки персональных данных стоит упомянуть о таких принципах, как законная и справедливая основа обработки персональных данных; целевой характер обработки персональных данных; обеспечение точности и достаточности персональных данных при их обработке, отказ от объединения баз персональных данных, обрабатываемых с разными целями, и некоторые другие. Целевой характер обработки персональных данных, в частности, предполагает необходимость

обработки только тех персональных данных, которые отвечают целям обработки; обеспечение соответствия содержания и объема обрабатываемых персональных данных заявленным целям обработки; воздержание от избыточной по отношению к заявленным целям обработки персональных данных; актуальность персональных данных применительно к целям обработки; соответствие срока хранения целям обработки персональных данных. Все обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом. Иные принципы обработки персональных данных закреплены также в ст. 86 Трудового кодекса РФ. Работодатели обязаны обеспечивать соблюдение этой нормы в своей деятельности.

Основными правовыми основаниями обработки персональных данных служат *согласие субъекта персональных данных на обработку; положения международного договора РФ или закона, договор, стороной, выгодоприобретателем или поручителем по которому выступает субъект персональных данных*, а также некоторые иные основания, упомянутые в ст. 6 Закона о персональных данных.

Интерес также представляет и такой предусмотренный Законом о персональных данных механизм, как поручение на обработку персональных данных. По общему правилу такое поручение может производиться оператором лишь с согласия субъекта персональных данных и должно содержать перечень действий (операций) с персональными данными, цели обработки, а также обязанности по обеспечению безопасности персональных данных. При этом само лицо, осуществляющее обработку персональных данных по поручению оператора, уже не обязано получать согласие субъекта персональных данных. В случае поручения обработки ответственность перед физическим лицом за действия указанного лица несет оператор.

Вопросы для дискуссии

1. Вопрос о защите персональных данных — юридический, скорее организационный либо по большей части технический? Как найти необходимый «баланс» мер столь разной природы?

2. Почему, несмотря на то что нормативное регулирование защиты персональных данных достаточно разветвленное, на практике остаются проблемы? Как юристы могут способствовать их решению?

3. Насколько достаточны и разумны меры ответственности, которые сегодня предусмотрены Законом о персональных данных и КоАП РФ за нарушение правил обработки персональных данных?

4. Каковы основные особенности защиты персональных данных, обрабатываемых посредством информационных систем?

5. Кто такой Data Protection Officer и каким требованиям должен отвечать лицо, замещающую такую должность в организации?

6. Насколько, на ваш взгляд, справедливо утверждение, что защита персональных данных — это удел крупных и финансово устойчивых организаций? Можете ли вы привести примеры организаций, система защиты персональных данных в которых близка к нормативному идеалу?

Задания

1. Ознакомьтесь с видеолекцией Т. Р. Суrowой «Понятие и виды персональных данных» и вставьте недостающие слова (фразы) в определение понятия «обработка персональных данных».

«Обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемых с использованием _____ или _____ с персональными данными, включая _____ персональных данных».

2. Ознакомьтесь с видеолекцией Т. Р. Суrowой «Принципы обработки персональных данных» и перечислите известные вам принципы обработки персональных данных.

3. Изучите ст. 86 Трудового кодекса РФ и укажите дополнительные обязанности (3 обязанности на выбор) по обработке персональных данных, которые возлагаются на оператора Трудовым кодексом РФ.

4. Ознакомьтесь с видеолекцией Т. Р. Суrowой «Документы оператора персональных данных» и перечислите требования, которые предъявляются к типовым формам или связанным с ними документам (карточки, анкеты, журналы), содержащим персональные данные.

5. Опираясь на положения ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», сформулируйте организационные меры обеспечения безопасности персональных данных.

6. Прослушайте подкаст Д. М. Мурина «Защита персональных данных в компании» и опишите алгоритм подготовки оператора к плановой проверке.

7. Прослушайте подкаст Т. Р. Суrowой «Проверки операторов персональных данных: как быть к ним готовым?» и перечислите основания

для проведения внеплановой проверки во взаимодействии на предмет соблюдения законодательства о персональных данных.

Задачи

1. Индивидуальный предприниматель Смирнов разработал веб-сервис, который обеспечивает возможность записи клиентов к зарегистрированным в сервисе компаниям, работающих в сфере услуг (красота, медицина, ветеринария и пр.). При регистрации пользователь «создает» свою компанию, сотрудников и перечень услуг. После этого ему становится доступной ссылка для записи онлайн, которую можно разместить как виджет сайта, и через него клиенты будут записываться на услуги. Клиента можно записать вручную (клиент звонит в компанию и диктует сотруднику свои данные), либо клиент записывается через систему записи онлайн и вводит свои данные (ФИО, номер телефона, аккаунт в соцсети и пр. данные, которые компания настроит для сбора в форме). После внесения данные сохраняются в базу Смирнова. Какая-либо регистрация клиентов в сервисе через создание своих аккаунтов не предусмотрена. Конечными получателями данных клиентов являются компании, оказывающие услуги, они же определяют и перечень собираемых данных клиентов.

Можно ли рассматривать Смирнова, владеющего сервисом, в качестве оператора персональных данных? Если да, то есть ли необходимость ему включаться в реестр операторов персональных данных Роскомнадзора? Какие рекомендации вы бы дали Смирнову по оптимизации его работы? Ответ аргументируйте.

2. Обычно системы по управлению персоналом (НСМ-системы) оперируют следующими данными:

- должность;
- стаж;
- подразделение сотрудника;
- ежегодные результаты оценки по компетенциям;
- ежегодная оценка результативности работы (KPI);
- результаты и длительность обучения на электронных курсах;
- результаты сдачи квалификационного тестирования;
- знания и навыки сотрудника;
- результативность и длительность выполнения сотрудником индивидуального плана развития.

Определите риски, которые могут возникнуть, если обозначенные в списке данные попадут в руки третьих лиц.

Как компаниям, использующим системы по управлению персоналом, можно перераспределить ответственность по обработке и хранению персональных данных?

3. Сотрудник Старовойтов передал свои учётные данные коллеге, чтобы тот успешно сдал за него квалификационное тестирование. По внутренним правилам организации сотрудника не допускают к работе до сдачи квалификационного тестирования. Факт передачи учётных данных подтверждается анализом переписки через рабочую почту.

Определите порядок действий компании в описанной ситуации. Применение каких превентивных мер позволит компании избежать подобных ситуаций в дальнейшем?

Тема 4. Правовое обеспечение информационной безопасности в сфере электронного документооборота и электронной коммерции

1. Понятие, юридическое значение и виды электронной подписи.
2. Правовые основы использования и защиты электронной подписи в современном документообороте.
3. Правовое обеспечение информационной безопасности в сфере обмена электронными документами и электронной переписки.
4. Правовое обеспечение информационной безопасности в сфере электронного маркетинга, интернет-торговли и электронных платежей.
5. Правовой режим защиты данных в сфере услуг связи, хостинга и обслуживания сайтов.

Введение в тему

Электронный документооборот представляет собой способ обмена и работы с документами, оригиналы которых формируются в электронном виде. Понятие электронного документа имеет различные интерпретации в российской юридической практике: существующие подходы различаются в зависимости от цели, для которой формируется электронный документ, и сферы, в которой он используется. В самом общем виде электронный документ может быть определен как представленная в электронной форме информация, пригодная для восприятия человеком с использованием ЭВМ, а также для передачи по информационным сетям.

В отдельных случаях законодатель предъявляет требование о подписании электронных документов электронной подписью. В силу нормативной дефиниции последняя представляет собой информацию в электронной форме, присоединенную к другой информации в электронной форме и используемой для определения лица, подписывающего информацию. Законодательство различает два основных вида электронной подписи — простую (ПЭП) и усиленную, которая может быть неквалифицированной (НЭП) и квалифицированной (КЭП). Оба вида подписей являются эквивалентом собственноручной, однако различаются они в нескольких аспектах.

Во-первых, в основе простой и усиленной электронных подписей лежат разные способы и средства формирования. В отличие от простой подписи, НЭП и КЭП создаются и проверяются при помощи криптографических средств преобразования информации с использованием открытого и закрытого ключей электронной подписи, которые генерируются на основе криптографии. Во-вторых, различаются и функции указанных видов подписей. Если ПЭП служит лишь для целей аутентификации лица, подписавшего документ, то НЭП и КЭП гарантируют неизменность документа после его подписания. Несмотря на схожесть НЭП и КЭП между собой (создаются при помощи программ шифрования, хранятся на физических носителях, выдаются удостоверяющими центрами), важным отличием этих видов подписей служит наличие или отсутствие сертификации ФСБ России. Программы для создания КЭП проходят сертификацию ФСБ, при этом ключ проверки электронной подписи указывается в квалифицированном сертификате. Подобное делает КЭП максимально защищенным и надежным видом электронной подписи.

Обеспечение информационной безопасности при выпуске и использовании электронной подписи достигается посредством реализации ряда нормативных правил, регламентированных в законодательстве об электронной подписи. Одно из наиболее важных — требование об идентификации удостоверяющими центрами личности заявителей, которые обращаются за получением сертификатов. Кроме того, в настоящее время существенно усложнены правила получения удостоверяющими центрами аккредитации, а также процедура получения КЭП индивидуальными предпринимателями и юридическими лицами, которым следует обращаться для этих целей в налоговые органы. Однако, помимо правовых мер, не стоит забывать и о технических средствах предосторожности при использовании электронной подписи — применение средств защиты компьютерных устройств, соблюдение правил хранения носителей электронной подписи, сохранение конфиденциальности ключа электронной подписи.

Сферы применения электронной подписи достаточно разнообразны. Так, ПЭП активно применяются в отношениях в области электронной коммерции (например, при подтверждении транзакций, в сфере онлайн-покупок/подписок и пр.). При этом особо выделяется тенденция расширения возможностей применения НЭП. Так, в 2021 г. в Трудовом кодексе РФ были урегулированы правила введения работодателями электронного документооборота и использования последнего в целях взаимодействия с работниками. В силу этой новации были созданы правовые основы использования НЭП в кадровом электронном документообороте организаций.

Рекомендуемые дополнительные источники

Литературные

1. Савельев, А. И. Электронная коммерция в России и за рубежом : правовое регулирование / А. И. Савельев. — Москва : Статут, 2014. — 543 с. — URL : <https://biblioclub.ru/index.php?page=book&id=448075>

2. Симонова, С. В. Актуальные направления совершенствования статуса информационных посредников в B2B-сегменте России / С. В. Симонова // Вестник Ярославского государственного университета им. П. Г. Демидова. Серия : Гуманитарные науки. — 2022. — № 1. — С. 92–99. — URL : https://elibrary.ru/download/elibrary_48083732_36729409.pdf

Нормативно-правовые

1. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // СЗ РФ. — 2003. — № 28, ст. 2895.

2. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // СЗ РФ. — 2011. — № 15, ст. 2036.

3. Федеральный закон от 22.11.2021 № 377-ФЗ «О внесении изменений в Трудовой кодекс РФ» // СЗ РФ. — 2021. — № 48, ст. 7947.

Юридическая практика

Постановление Пленума Верховного Суда РФ от 26.12.2017 № 57 «О некоторых вопросах применения законодательства, регулирующего использование документов в электронном виде в деятельности судов общей юрисдикции и арбитражных судов» // Российская газета. — 2017. — 29 дек.

Вопросы для дискуссии

1. Что представляет собой электронный документооборот в современной компании и каковы его возможности? Как вы видите основные

вызовы ЭДО в аспекте информационной безопасности и обращает ли законодатель на эти проблемы внимание?

2. Каковы наиболее востребованные и актуальные сферы применения электронной подписи? Как работает электронная подпись с технической точки зрения?

3. В чем суть законодательных изменений относительно нового порядка получения и использования электронной подписи, введенных законом от 27.12.2019? Как можно оценить эти изменения с точки зрения их влияния на повышение безопасности ЭДО?

4. Каковы основные способы получения электронной подписи и подтверждения личности её владельца?

5. Каковы основные правила и требования к информационной безопасности при использовании электронной подписи? Как обеспечивается защита хранения и передачи информации в ЭДО и каким образом защищаются носители электронной подписи? Насколько безопасно дистанционное получение квалифицированной электронной подписи?

Задания

Прослушайте подкаст компании «Тензор» на тему «Электронные подписи в сфере информационной безопасности» и выполните следующие задания.

1. Перечислите известные вам виды электронной подписи.

2. Укажите основные сферы применения:

- неквалифицированной электронной подписи;
- квалифицированной электронной подписи.

3. Укажите, в каких случаях усиленную подпись необходимо получать:

- а) в налоговом органе;
- б) в удостоверяющем центре;
- в) в Центральном банке РФ;
- г) в удостоверяющем центре Федерального казначейства.

4. Укажите известные вам способы получения электронной подписи через удостоверяющий центр.

5. Перечислите основные правила безопасности, которые следует учитывать владельцу электронной подписи при её использовании.

Прослушайте подкаст компании «DrCash» «Угрозы информационной безопасности в работе партнерских сетей» и выполните задания.

6. Дайте определение партнерской сети.

7. Укажите известные вам угрозы информационной безопасности, актуальные для рынка СРА-маркетинга и партнерских сетей в целом.

Задача

Перед компанией стоит задача ознакомить в электронном виде своих сотрудников с локальными актами и документами (в том числе по вопросам обработки и защиты персональных данных). Процедура ознакомления должна отвечать следующим признакам: 1) быть юридически грамотной и влекущей юридические последствия; 2) позволять вести учет работников, подлежащих ознакомлению; 3) обеспечивать возможность оперативного контроля работодателем результатов ознакомления с выявлением работников, не прошедших своевременно процедуру ознакомления.

Оцените ситуацию. Какие варианты решения стоящей перед компанией задачи вы бы предложили как юристы? Что важно будет учесть в случае, если проблема будет решаться на уровне разработки специальной информационной системы?

В случае если вопрос о том, ознакомился ли работник с документами, будет поднят в суде, какие доказательства необходимо предоставить работодателю? Возникают ли у работодателя какие-либо юридические риски в случае, если: 1) работник умышленно заявляет, что не ознакомился с документами, хотя ознакомление имело место; 2) работник действительно не ознакомился с документами, хотя должен был это сделать; 3) сотрудник заявляет, что работодатель изменил текст документов, с которыми был ознакомлен сотрудник.

Если риски есть, то как вы предложили бы их нивелировать?

Тема 5. Правовое обеспечение информационной безопасности в области интеллектуальной собственности

1. Интеллектуальная собственность и информационная сфера.
2. Регулирование объектов авторского права в сети «Интернет».
3. Юридические аспекты защиты инфопродуктов.
4. Программа для ЭВМ как объект авторского права.
5. Базы данных как объект авторского права.
6. Информационная безопасность в сфере лицензионных договоров.
7. Правовая охрана товарных знаков.

Дополнительная литература

1. Право интеллектуальной собственности. Международно-правовое регулирование : учеб. пособие для бакалавриата и магистратуры / отв. ред. Г. И. Тыцкая. — Москва : Юрайт, 2019. — 252 с. — URL : <https://urait.ru/bcode/438995>

2. Вишнякова, И. В. Авторское право : учеб. пособие И. В. Вишнякова. — Казань : Казанский национальный исследовательский технологический университет, 2017. — 112 с. — URL : <http://www.iprbookshop.ru/79259.html>

3. Право интеллектуальной собственности : учеб. для вузов / под ред. Л. А. Новоселовой. — Москва : Юрайт, 2019. — 343 с. — URL : <https://urait.ru/bcode/444530>

4. Калятин, В. О. Право интеллектуальной собственности. Правовое регулирование баз данных : учеб. пособие для вузов / В. О. Калятин. — Москва : Юрайт, 2022. — 186 с. — URL : <https://urait.ru/bcode/493351>

5. Радецкая, М. В. Обзор судебной практики по вопросу взыскания компенсации за нарушение исключительного права на результат интеллектуальной деятельности или средство индивидуализации / М. В. Радецкая, А. Е. Туркина // Журнал Суда по интеллектуальным правам. — 2020. — № 27. — С. 5–40. — URL : <http://ipcmagazine.ru/legal-issues/review-of-judicial-practice-on-the-issue-of-recovering-compensation-for-violation-of-the-exclusive-right-to-the-result-of-intellectual-activity-or-means-of-individualization>

Информационные источники

1. Антонец, В. А. Онлайн-курс «Коммерциализация результатов НИОКР» / В. А. Антонец. — URL : <https://www.coursera.org/learn/kommercializaciya-niokr?action=enroll>
2. Linkmark — информационная база данных. — URL : <https://linkmark.ru/>
3. Официальный сайт CreativeCommons. — URL : <https://creativecommons.org/>
4. Локарнская классификация — сайт ВОИС. — URL : <https://www.wipo.int/classifications/locarno/ru/>
5. Калькулятор пошлин. — сайт ВОИС. — URL : <https://www.wipo.int/hague/en/fees/calculator.jsp>
6. Бернская конвенция по охране литературных и художественных произведений от 9 сентября 1886 г., измененная 28 сентября 1979 г. — URL : <https://wipolex.wipo.int/ru/text/283697>
7. Нормативные документы о программах для ЭВМ и базах данных. — URL : <https://www.fips.ru/to-applicants/software-and-databases/programmy-dlya-evm-bd-normativnye-dokumenty.php>
8. Средства индивидуализации. Товарные знаки. Нормативные документы — URL : <https://www.fips.ru/to-applicants/trademarks/tovarnye-znaki-znaki-obsluzhivaniya-i-naimenovaniya-mest-proiskhozhdeniya-tovarov-normativnye-dokume.php>
9. Ассоциация ЦПТИ. — URL : <https://www.youtube.com/channel/UCkLjDZ4CgAdcsEodmRHw4Dg>

Юридическая практика

1. Постановление Пленума Верховного Суда РФ от 23.04.2019 № 10 «О применении части четвертой Гражданского кодекса Российской Федерации» // Российская газета. — 2019. — 6 мая.
2. Обзор судебной практики по делам, связанным с разрешением споров о защите интеллектуальных прав // Бюллетень Верховного Суда. — 2015. — № 11.

Введение в тему

Интеллектуальная собственность в самом широком смысле — результат творческой деятельности человека. Право интеллектуальной собственности обеспечивает охрану прав авторов и правообладателей результатов интеллектуальной деятельности. Отдельные виды интеллектуальной деятельности регулируются нормами международного права,

нормами национального законодательства каждой страны, иными нормативными актами. В числе основных международных актов, ратифицированных нашей страной, можно отметить Бернскую конвенцию об охране литературных и художественных произведений (1886 г.), Соглашение по торговым аспектам прав интеллектуальной собственности (ТРИПС) (принято в 1995 г.), Договор об авторском праве (ДАП) (так называемый «Договор ВОИС в области Интернета») 1996 г., Договор по исполнениям и фонограммам (ДИФ) 1996 г.

Договоры ДАП и ДИФ стали первыми документами, которые регулировали режим охраны произведений и прав их авторов в цифровой среде. Они прямо указывали на то, что компьютерные программы и базы данных выступают объектами авторского права. Основной целью правового регулирования отношений в интеллектуальной сфере является обеспечение баланса между интересами создателей контента, разработчиков и правообладателей, с одной стороны, и интересами общества в плане доступа к творческим произведениям — с другой стороны.

Объекты авторского права в РФ регулируются в большей степени положениями части 4 Гражданского кодекса РФ (далее — ГК РФ). Охраняемые результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации перечислены в ст. 1225 ГК РФ. Следует обратить внимание на то, что автор — человек, творческим трудом которого создано произведение. Автором не может выступать юридическое лицо или государственный орган. В соответствии со ст. 1300 ГК РФ лицо, указанное в качестве автора на экземпляре произведения либо иным образом, считается его автором, если не доказано иное. Оказание третьими лицами финансового, организационного, технического содействия автору в процессе создания произведения не порождает авторства произведения.

Правообладатель — это физическое или юридическое лицо, обладающее имущественными правами на объект интеллектуальной собственности. Первоначально автор является правообладателем, далее правообладателем могут быть наследники, работодатели, издатели, лица, права к которым перешли на основании договора (отчуждения прав, лицензионного договора).

Авторское право распространяется на произведения независимо от их назначения и достоинства, а также от способа выражения (ст. 1259 ГК РФ). Таким образом, законодательство не делает различий между высокохудожественными и иными произведениями. Критерием охраноспособности произведений, помимо их творческого характера, служит объективная форма выражения произведения. Идеи и мысли физического лица

не охраняются до тех пор, пока её не имеют. В силу прямого указания закона авторское право не распространяется на идеи, методы, процессы, системы, способы, концепции, принципы, открытия, факты, языки программирования.

Права автора на произведение могут иметь как личную неимущественную, так и имущественную природу (исключительные права). Личные неимущественные права принадлежат автору произведения независимо от того, как он распорядился имущественными правами, и охраняются бессрочно.

В статьях 1273, 1274, 1276 ГК РФ предусмотрены возможности для правомерного использования произведений/информации без выплаты вознаграждения автору/правообладателю. Кроме того, существует специальный режим использования произведений библиотеками и архивами (ст. 1275 ГК РФ).

Существует несколько способов защиты объектов авторского права, например посредством размещения на произведении значка © (copyright), который служит уведомлением о том, что объект охраняется авторским правом. Еще одним способом являются технические средства защиты (DRM) (ст. 1299 ГК РФ). Авторы самостоятельно могут хранить депозитарий со своими произведениями, довольно популярным в настоящее время средством защиты является депонирование.

Следует уделить особое внимание таким объектам, как программы для ЭВМ и базы данных. В международных актах не дается четкого определения компьютерных программ в силу того, что это очень быстро меняющийся объект. Единственно возможный критерий оригинальности компьютерных программ связан с тем, что они должны представлять собой результат интеллектуального творчества автора.

Иное дело — база данных. В ст. 5 Договора ДАП дается четкое указание, что «база данных — компиляция данных или другой информации в любой форме, которые по подбору и расположению материалов представляют собой результат интеллектуального творчества».

В гражданском законодательстве компьютерным программам также дано определение (ст. 1261 ГК РФ). В соответствии с ГК РФ правовая охрана распространяется на все виды программ для ЭВМ, которые могут быть написаны на любом языке и в любой форме, включая исходный текст и объектный код. Правовая охрана не распространяется на идеи и принципы, лежащие в основе программы для ЭВМ, базы данных, или какого-либо их элемента, в том числе на идеи и принципы организации интерфейса и алгоритма, а также на языки программирования.

База данных — сложный объект, поскольку может включать в себя материалы, охраняемые как авторским правом, так и смежным правом. Базы данных, в отличие от программ для ЭВМ, охраняются еще и как объекты смежного права. Определение баз данных дано в ст. 1260 ГК РФ. Для них, как и для программ для ЭВМ, важным критерием является оригинальность и творческий вклад автора.

Дополнительной защитой для таких объектов является возможность государственной регистрации. Государственная регистрация производится путем подачи заявки в ФИПС. Преимуществом такой регистрации является то, что сведения вносятся в Государственный реестр программ для ЭВМ / баз данных, правообладателю выдается свидетельство, в котором указана дата регистрации, авторы, имя правообладателя, название объекта. В случае если возникнут какие-либо споры о принадлежности программы для ЭВМ / базы данных, факт такой регистрации будет служить доказательством прав на объект.

Для индивидуализации на рынке и защиты бренда производители товаров, работ, услуг используют средства индивидуализации. К таковым относятся фирменное наименование, коммерческое обозначение, товарный знак / знак обслуживания, географическое указание (ГУ), наименование места происхождения товара (НМПТ).

Одним из самых популярных средств индивидуализации является товарный знак. Международное регулирование таких объектов образуют Парижская конвенция по охране промышленной собственности (1883 г.), Ниццкое соглашение о международной классификации товаров и услуг для регистрации знаков (1957 г.), Мадридское соглашение (1891 г.) и Протокол к нему (1989 г.).

В РФ правовой режим товарных знаков определяется частью 4 ГК РФ. Товарный знак / знак обслуживания — обозначение, служащее для индивидуализации товаров юридических лиц или индивидуальных предпринимателей (ст. 1477 ГК РФ). В качестве товарных знаков могут быть зарегистрированы словесные, изобразительные, объемные и другие обозначения или их комбинации (ст. 1482 ГК РФ), товарный знак может быть зарегистрирован в любом цвете или цветовом сочетании.

Товарный знак подлежит государственной регистрации. Регистрация осуществляется на основании заявки, которая может быть подана как в бумажном, так и в электронном виде в ФИПС. Заявка должна содержать следующие элементы: заявление, заявляемое обозначение, перечень товаров/услуг в отношении которых испрашивается регистрация в соответ-

ствии с Международной классификацией товаров и услуг (МКТУ), описание заявляемого обозначения.

Товарный знак / знак обслуживания удостоверяет исключительное право правообладателя на использование соответствующего обозначения в отношении перечня товаров/услуг, указанных в свидетельстве, и действует 10 лет с возможностью продления еще на 10 лет неограниченное количество раз. Товарный знак выполняет ряд таких функций, как рекламная, отличительная, охранительная, эстетическая, стимулирующая и защитная.

В РФ наблюдается устойчивый рост числа заявок на регистрацию товарных знаков. Согласно статистике Роспатента, в 2021 г. было подано свыше 100 000 заявок на регистрацию, соответственно растёт и количество зарегистрированных товарных знаков. Исследователи связывают такой рост с импортозамещением в нашей стране, а также с повышением уровня знаний в сфере интеллектуальной собственности.

Задачи

1. Посмотрите видеолекцию Е. Н. Мазалецкой «Интеллектуальная собственность и информационная сфера» и решите задачу.

Гражданин Петров создал произведение, которое в дальнейшем планирует передать в издательство для опубликования. При этом автор опасается, что его авторские права будут нарушены со стороны издательства или читателей.

Дайте юридическую консультацию автору. Что является основанием возникновения права на авторство и как его гарантировать?

2. Посмотрите видеолекцию Е. Н. Мазалецкой «Программы для ЭВМ как объект авторского права» и решите задачу.

Гражданин Авоськин разработал программу для ЭВМ, которая может распознавать поведение людей. Охранное предприятие изъявило желание приобрести исключительные права на данную программу.

Какой договор нужно составить в данном случае? Может ли Авоськин отказаться передать исключительное право в полном объёме?

3. Посмотрите видеолекцию Е. Н. Мазалецкой «Базы данных как объект авторского права» и решите задачу ниже.

Сотрудники института собирали базу питания учащейся молодежи и собрали большую базу, на основе которой составляли оптимальный рацион питания учащихся.

Обязаны ли они зарегистрировать данный результат интеллектуальной деятельности? Каким образом охраняется база данных?

4. Посмотрите видеолекцию Е. Н. Мазалецкой «Регулирование объектов авторского права в сети «Интернет» и решите задачу.

Гражданин Морковкин собирает и публикует на своём сайте в сети «Интернет» литературные произведения, написанные как классиками отечественной и зарубежной литературы, так и современными авторами. При этом он указывает название и автора произведения.

Насколько правомерны указанные действия?

5. Компания «Л» предоставляет заказчикам доступ к программному продукту В. по договору аренды. При этом физически программное обеспечение располагается на серверах сторонней компании «Х», с которой ООО «Л» заключила договор. В марте 2022 г. серверы компании «Х» подверглись DDOS-атаке, что повлекло сбой в работе сервиса, при котором пользователи в течение трёх дней получали нестабильный доступ к сервису.

Каким образом можно обезопасить компанию «Л» от указанных в задаче рисков?

Задания

1. Прослушайте подкаст Е. Н. Мазалецкой «Информационная безопасность в сфере лицензионных договоров» и назовите виды лицензионных договоров. Укажите, в какой форме заключается лицензионный договор.

2. Дайте определение товарного знака. Объясните, чем отличается товарный знак от фирменного наименования? Составьте сравнительную таблицу, где укажите сходства и различия товарного знака и фирменного наименования.

Тема 6. Информационная безопасность в социальной сфере и при применении отдельных цифровых технологий

1. Понятие и виды информации, причиняющей вред здоровью и развитию несовершеннолетних.

2. Порядок и механизмы информационной защиты несовершеннолетних.

3. Правовое обеспечение информационной безопасности в системе государственных и муниципальных электронных услуг.

4. Правовое обеспечение информационной безопасности при ведении публичных электронных реестров.

5. Правовое обеспечение информационной безопасности при использовании технологии блокчейн, облачных сервисов и искусственного интеллекта.

6. Защита информационной безопасности инвестиционных платформ, краудфандинга, краудинвестинга и механизмов ICO.

Рекомендуемые дополнительные источники

Литературные

1. Ефимова, Л. Л. Правовое регулирование информационной безопасности детей как новый правовой институт информационного права / Л. Л. Ефимова // Аграрное и земельное право. — 2018. — № 6. — С. 131–138. — URL : <https://www.elibrary.ru/item.asp?id=36355736>

2. Симонова, С. В. Информационная безопасность несовершеннолетних в цифровой среде : материально-правовые и процессуальные вопросы / С. В. Симонова // Социально-юридическая тетрадь. — 2020. — № 10. — С. 26–37. — URL : <https://www.elibrary.ru/item.asp?id=44299888>

Нормативно-правовые

1. Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» // СЗ РФ. — 2010. — № 31, ст. 4179.

2. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ. — 2011. — № 1, ст. 48.

3. Федеральный закон от 18.03.2019 № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» // СЗ РФ. — 2019. — № 12, ст. 1224.

4. Федеральный закон от 02.08.2019 № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. — 2019. — № 31, ст. 4418.

5. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. — 2020. — № 31 (Ч. I), ст. 5018.

6. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // СЗ РФ. — 2019. — № 41, ст. 5700.

7. Распоряжение Правительства РФ от 19.08.2020 № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // СЗ РФ. — 2020. — № 35, ст. 5593.

Введение в тему

В российском законодательстве под информационной безопасностью детей мыслится такое их состояние защищенности, при котором отсутствует риск причинения информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию. При этом под «вредоносной» информацией понимаются такие сведения, распространение которых запрещено или ограничено среди детей.

Обращает на себя внимание, что нормативная дефиниция информационной безопасности ребенка выводит за пределы правовой охраны персональные данные детей, которые нередко являются одним из основных объектов посягательств в цифровой среде. Кроме того, законодатель не дает объективных критериев, которые можно было бы использовать в правоприменительной практике в целях определения тех или иных сведений в качестве запрещенных и причиняющих вред личности несовершеннолетнего.

В целом одними из основных правовых средств обеспечения информационной безопасности детей в Федеральном законе от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» являются такие механизмы, как определение перечня запрещенной и ограниченной среди детей информации (ст. 5 закона), правила классификации информационной продукции (ст. 6–10 закона), правила оборота информационной продукции, в том числе в сети «Интернет» (ст. 11–16 закона). В то же время многое в сфере защиты детей от «вредной информации» находится по-прежнему за пределами правового регулирования. В частности, отсутствуют специальные нормативные правила работы IT-отрасли и цифровых платформ в целях защиты прав детей, особые процедуры получения согласия несовершеннолетнего на обработку его персональных данных, требования к каналам распространения онлайн-рекламы и к онлайн-играм с позиции особенностей интересов несовершеннолетних.

Говоря об обеспечении защиты информации при применении современных цифровых технологий, особое внимание следует уделить таким технологиям, как блокчейн, искусственный интеллект и облачные технологии. Применение этих технологий само по себе повышает гарантии кибербезопасности сохранности данных. В то же время при разработке и использовании этих технологий важно учитывать предусмотренные российским законодательством общие правила оборота и обработки данных, защиты информационных прав граждан.

Вопросы для дискуссии

1. Каким образом вы видите решение проблемы кибербуллинга в России? Какие законодательные реформы могли бы повысить гарантии защиты детей от агрессии, запугивания и травли в сети «Интернет»?

2. Как вы смотрите на инициативу введения минимального возраста использования социальных сетей и усложнения процедуры регистрации в них несовершеннолетних?

3. Каким образом гарантировать с практической точки зрения ограничение возможности посещения несовершеннолетними сайтов с запрещенной для их возраста информацией?

4. Имеются ли основания и механизмы привлечения родителей к юридической ответственности за потребление их детьми запрещенной информации, посещение запрещенных сайтов, распространение противозаконного контента?

5. Какие законодательные инициативы, на ваш взгляд, могут способствовать повышению гарантий информационной безопасности при применении отдельных цифровых технологий?

Задача

Гражданка Иванова опубликовала в своем личном аккаунте социальной сети «ВКонтакте» фотографии 10-летней дочери Марии. Узнав об этом, отец Марии потребовал удалить размещенные снимки, ссылаясь на то, что он как родитель возражает против распространения фотографий своего ребенка. Тем более что публикация фотографий из семейного архива вызвала у дочери большое смущение. Иванова не согласилась с отцом Марии, указав на то, что она является законным представителем ребенка и действует в его интересах. Иванова подчеркнула, что, опубликовав фото, она тем самым дала согласие на обработку персональных данных своего ребенка.

Оцените ситуацию.

Контрольные вопросы

1. Информация как объект социально-экономических отношений. Базовые понятия права информационной безопасности.
2. Основные виды информационных угроз в социальной и экономической сферах и юридические механизмы их нейтрализации.
3. Понятие, юридические средства и система мер обеспечения информационной безопасности в социальной и экономической сферах.
4. Национально-правовые и международные основы обеспечения информационной безопасности в социальной и экономической сферах.
5. Основания и порядок ограничения доступа к информации в социальной и экономической сферах.
6. Ответственность за нарушения в сфере оборота информации при реализации социальных и экономических прав.
7. Конфиденциальность информации и механизмы её обеспечения.
8. Понятие и виды персональных данных.
9. Основания и принципы обработки персональных данных при реализации социальных и экономических прав.
10. Основные документы операторов персональных данных.
11. Понятие и правовой режим коммерческой тайны.
12. Правовой режим служебной и профессиональной тайны.
13. Право на секрет производства (ноу-хау).
14. Понятие и виды информации, причиняющей вред здоровью и развитию детей.
15. Порядок и механизмы информационной защиты несовершеннолетних.
16. Использование систем распределенных реестров в социальной и экономической сферах: перспективы и правовые основы.
17. Правовое обеспечение информационной безопасности при использовании технологии блокчейн.
18. Применение искусственного интеллекта в социальной и экономической сферах: правовые проблемы информационной безопасности.
19. Понятие, юридическое значение и основные виды электронной подписи.
20. Теоретические и практические вопросы защиты прав и законных интересов владельцев электронной подписи.
21. Правовое обеспечение информационной безопасности в сфере обмена электронными документами и электронной переписки.

22. Правовой режим электронного обмена данными и электронных сделок.

23. Правовое обеспечение информационной безопасности в сфере электронного маркетинга, интернет-торговли и электронных платежей.

24. Интеллектуальная собственность и информационная сфера.

25. Регулирование объектов авторского права в сети «Интернет».

26. Правовой режим программ для ЭВМ и мобильных приложений.

27. Понятие и правовой режим баз данных.

28. Информационная безопасность в сфере услуг связи, хостинга и обслуживания интернет-сайтов.

Оглавление

О курсе «Правовое обеспечение информационной безопасности в социальной и экономической сферах»	3
Тема 1. Понятие и правовые основы информационной безопасности в социальной и экономической сферах	7
Тема 2. Режим конфиденциальности информации	13
Тема 3. Правовое обеспечение безопасности персональных данных	19
Тема 4. Правовое обеспечение информационной безопасности в сфере электронного документооборота и электронной коммерции	26
Тема 5. Правовое обеспечение информационной безопасности в области интеллектуальной собственности	31
Тема 6. Информационная безопасность в социальной сфере и при применении отдельных цифровых технологий	37
Контрольные вопросы	41

Учебное издание

Симонова Снежана Владимировна

Мазалецкая Елена Николаевна

**Правовое обеспечение
информационной безопасности
в социальной и экономической сферах**

Учебно-методическое пособие

Редактор, корректор М. Э. Левакова

Верстка М. Э. Леваковой

Подписано в печать 13.06.2023. Формат 60×84 1/16.

Усл. печ. л. 2,56. Уч.-изд. л. 2,0.

Тираж 2 экз. Заказ

Оригинал-макет подготовлен
в редакционно-издательском отделе ЯрГУ.

Ярославский государственный университет им. П. Г. Демидова.
150003, Ярославль, ул. Советская, 14.