СБЕР
КИБЕР
БЕЗОПАСНОСТЬ

SBER PRIVACY JOURNAL

Журнал DPO о персональных данных
и приватности

SIEM-СИСТЕМА КАК ИНСТРУМЕНТ ЗАЩИТЫ ДАННЫХ

КЛЮЧЕВЫЕ АСПЕКТЫ РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ДАННЫМИ

ТРЕНДЫ РЕГУЛИРОВАНИЯ БИОМЕТРИИ

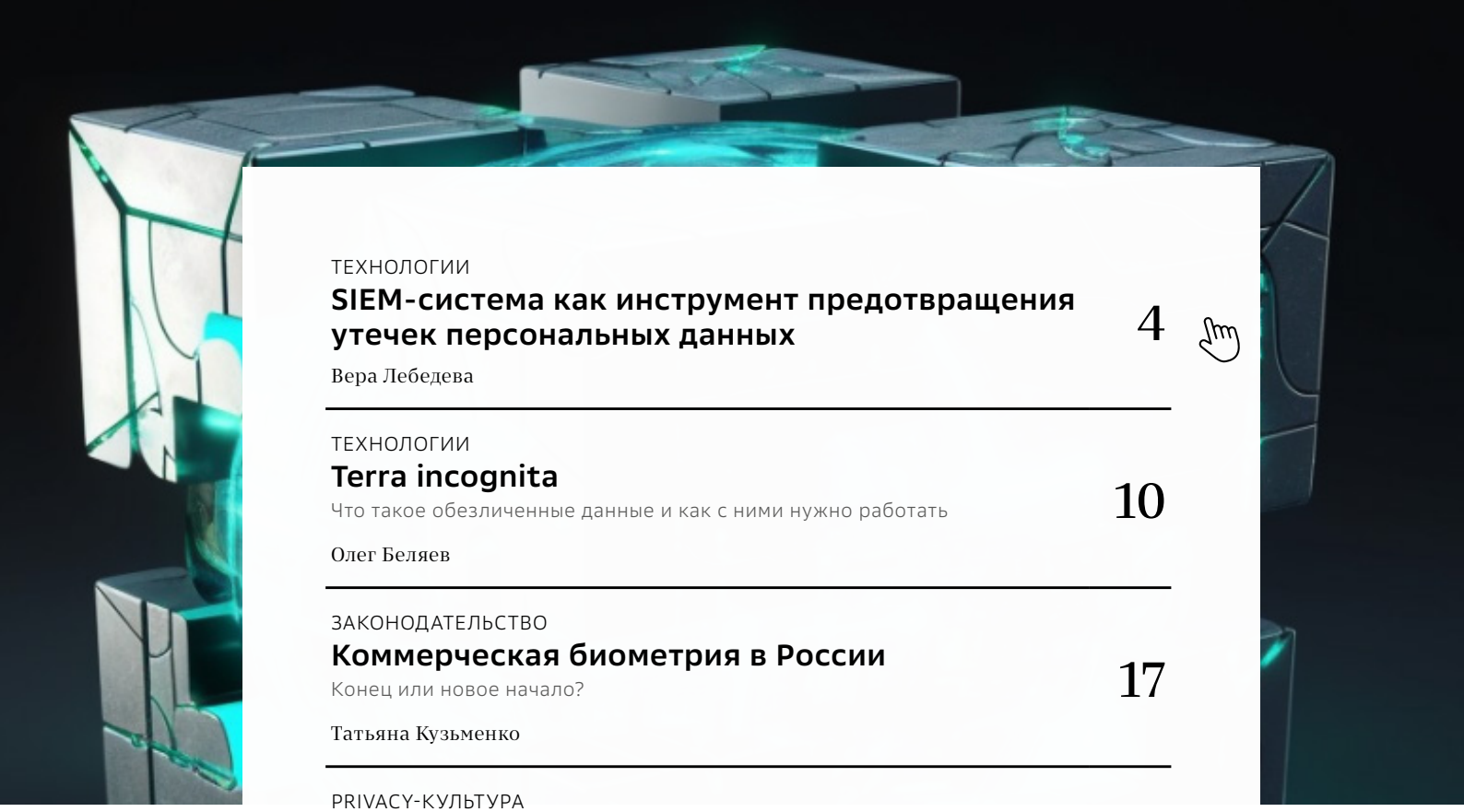
БЕЗОПАСНОСТЬ ДЕТЕЙ В ОНЛАЙН-ИГРАХ

СЕКРЕТЫ ПОВЫШЕНИЯ PRIVACY-КУЛЬТУРЫ РАБОТНИКОВ

РЕКОМЕНДАЦИИ ПО ОБРАБОТКЕ ДАННЫХ, ПОЛУЧЕННЫХ В ХОДЕ ТЕЛЕФОННОГО РАЗГОВОРА

ВЫПУСК №6 | СЕНТЯБРЬ 2023

SBER PRIVACY JOURNAL



СОДЕРЖАНИЕ

SIEM-система как инструмент предотвращения утечек персональных данных

Главной отличительной чертой XXI века, века информационных технологий, стало применение интернета в деятельности каждой компании. С этого времени, день ото дня, угрозы информационной безопасности растут, а рост атак происходит как с точки зрения их количества, так и сложности. На восприимчивость компаний к кибератакам влияет не только рост численности кибернарушителей, но и доступные им инструменты, которые становятся все более изощренными.

Современная ИТ-инфраструктура компании состоит из множества корпоративных систем, которые обрабатывают различные виды конфиденциальной информации, в том числе персональные данные. Чем больше различного программного обеспечения используется в информационной системе, тем больше вероятность возникновения утечек персональных данных, связанных со взломом программного обеспечения или несанкционированной передачей персональных данных (вследствие наличия уязвимостей, вирусов, неточностей и нарушений в программном коде), а также обходом или преодолением элементов защиты.

Немного фактов

- Роскомнадзором с начала 2023 года было получено **177** уведомлений от компаний об утечках персональных данных, из них подтверждено почти **70** случаев[1].
- Согласно исследованию «РТК-Солар», в открытом доступе находится **340 млн** учетных записей россиян[2].
- Как ранее было отмечено в одной из статей[3], с учетом большого количества утечек «пробить» персональные данные через telegram-бот или купить базу персональных данных в даркнете не составляет особого труда. «Базовый» набор персональных данных, состоящий из ФИО, номера телефона и e-mail, который используется для регистрации в сервисах, можно «пробить» бесплатно, а за получение особо чувствительной категории персональных данных, среди которых номер банковской карты, сведения о транзакциях, диагнозе, результаты анализов, необходимо заплатить злоумышленникам всего лишь несколько десятков тысяч рублей.
- Утечки конфиденциальной информации из коммерческих компаний и государственных органов являются основным источником получения персональных данных злоумышленниками.

В связи с участившимися случаями взлома баз персональных данных компании должны постоянно следить за безопасностью информации в ИТ-инфраструктуре. Но, как уже говорилось ранее, из-за большого количества компонентов в информационной системе, которые фиксируют колоссальные объемы данных о различных событиях в журналах аудита информационных систем, без автоматизированного инструмента невозможно оперативно обработать всю протоколируемую информацию и принять своевременные меры по локализации возможных угроз безопасности персональных данных.

Для того, чтобы обеспечить защиту персональных данных и иной конфиденциальной информации, специалисты кибербезопасности используют SIEM (Security information and event management) – систему управления информацией о безопасности и событиями безопасности, которая позволяет централизованно обрабатывать данные журналов регистрации событий, поступающих из различных информационных систем, тем самым повышая уровень защиты персональных данных в компании. SIEM-системы используются для построения центров мониторинга информационной безопасности (SOC, Security Operations Center)[4].

Разберем подробнее, что такое SIEM

SIEM – это технология, предназначенная для сбора и анализа информации о событиях безопасности. Аббревиатура SIEM[5] объединяет в себе две концепции: управление информацией о безопасности (SIM) и управление событиями безопасности (SEM). Под первой понимается сбор, хранение и анализ исторических данных, относящихся к безопасности, под второй – процесс мониторинга и анализа событий безопасности в режиме реального времени, позволяющий устранить угрозы, выявить закономерности и реагировать на инциденты. SEM-система тщательно следит за определенными событиями, которые могут требовать незамедлительного реагирования.

Таким образом, решение SIEM объединяет возможности этих двух подходов в одну централизованную систему.

[1] Роскомнадзор подтвердил почти 70 сигналов об утечках персональных данных. Интерфакс. URL: https://www.interfax.ru/russia/904565 (дата обращения 27.09.2023).

[2] В открытом доступе находится 340 млн. учетных записей россиян. RSpectr. URL: https://rspectr.com/novosti/v-otkrytom-dostupe-nahoditsya-340-mln-uchetnyh-zapisej-rossiyan; РТК «Солар». Отчет о ключевых внешних цифровых угрозах для российских компаний в январе-апреле 2023 года. URl: https://rt-solar.ru/analytics/reports/3452/ (дата обращения 27.09.2023).

[3] «Пробив» – это противозаконная услуга, с помощью которой злоумышленники получают из имеющихся источников информацию о конкретных людях. Подробнее про анализ теневого рынка персональных данных читайте в 4-м выпуске Sber Privacy Journal. URL: http://www.sberbank.ru/common/img/uploaded/kibrary/dpo/sbp_journal_vol4.pdf (дата обращения 27.09.2023).

[4] В частности, SIEM используется SOC СберБанка и иными компаниями, которые предоставляют услуги обеспечения информационной безопасности.

[5] Что такое SIEM? Microsoft Security. URL: https://www.microsoft.com/ru-ru/security/business/security-101/what-is-siem (дата обращения 27.09.2023).

Путь развития SIEM

Эволюция SIEM происходила благодаря крупным компаниям, которые нуждались в автоматизированном и комплексном инструменте обнаружения угроз информационной безопасности в режиме реального времени. Из-за стремительного увеличения объемов данных, обрабатываемых системой, SIEM с течением времени совершенствовались. Для того, чтобы понять всю «мощь» данного решения, проследим как оно развивалась.

Появление ***первого поколения***[6] SIEM-систем в 2005 году открыло новые возможности в области защиты данных. Впервые объединив в себе управление событиями безопасности с управлением информацией о безопасности, которые ранее были разделены, SIEM-система позволила специалистам кибербезопасности стать более эффективными при работе в сложных ИТ-инфраструктурах. Однако первые системы имели ряд недостатков. Они плохо масштабировались, были ограничены в сложности создаваемых ими оповещений и страдали плохой визуализацией. Также каждый этап процесса мониторинга и реагирования требовал ручного вмешательства специалистов.

Главным отличием SIEM-систем ***второго поколения*** стала возможность масштабирования. Также были улучшены отчеты и информационные панели мониторинга. Хранение данных длительное время в SIEM первого поколения было не востребовано, поскольку система не могла эффективно запрашивать данные архивных событий (от нескольких недель). Появление масштабируемых систем хранения данных позволило SIEM второго поколения использовать анализ больших данных. Это означало, что теперь данные могли запрашиваться за гораздо более длительный период. Следовательно, система имела больше данных для формирования событий по инцидентам, что повысило вероятность их обнаружения и возможности реагирования на них.

Соответственно, первое поколение SIEM-систем предоставило специалистам кибербезопасности возможность быть эффективными, однако второе поколение отняло эту возможность, предоставив больше данных, чем они могли обработать.

В развитие ***третьего поколения*** SIEM-систем внес свой вклад анализ поведения пользователей и объектов (UEBA, User and Entity Behavior Analytics). UEBA[7] использует инновационные аналитические технологии, включая алгоритмы машинного обучения, что позволяет выявлять потенциально опасное поведение пользователей и устройств. UEBA расширил видимость SIEM-систем с помощью своих возможностей обнаружения инцидентов. Данная технология способна определять события безопасности, которые другими средствами защиты не определяются в силу их несоответствия предопределенным правилам, настроенным на таких средствах защиты.

> Таким образом, SIEM-система нового поколения – это не просто сумма двух ее начальных частей – SIM и SEM, это мощный и эффективный инструмент для обеспечения информационной безопасности.

[6] Поколения SIEM. URL: https://www.exabeam.com/explainers/siem-security/a-siem-security-primer/ (дата обращения 27.09.2023).

[7] Что такое UEBA? URL: https://encyclopedia.kaspersky.ru/glossary/ueba/ (дата обращения: 27.09.2023)

Технология и значимость SIEM

SIEM были разработаны для того, чтобы помочь специалистам кибербезопасности управлять событиями из различных источников. На эффективность работы SIEM-системы влияют ее функциональные возможности. Рассмотрим основные из них:

Количество источников данных

Одной из главных особенностей SIEM-системы является возможность сбора информации из множества разнообразных источников данных в ИТ-инфраструктуре. Как правило, это могут быть как «активные» источники, которые передают данные в SIEM самостоятельно, так и «пассивные», к которым SIEM-система обращается сама.

Правила корреляции

Правила корреляции предполагают соотнесение между собой событий, удовлетворяющих тем или иным условиям. Корреляция помогает специалистам кибербезопасности осмыслить и понять огромное количество собираемых данных и отфильтровать те, которые могут быть потенциально опасными. Успех формирования инцидентов информационной безопасности в SIEM-системе зависит от «силы» правил корреляции.

Объем обрабатываемых данных

Анализ больших объемов данных, собираемых из различных источников, необходим для получения более полной информации о событиях и улучшения мониторинга. Для результативности работы SIEM важна возможность системы поддерживать большие объемы данных, которые нужны для корреляции событий и их хранения.

Производительность

Система, обрабатывающая большой объем данных, не сможет работать оперативно, если отдельные процессы будет выполняться слишком долго, а для минимизации последствий инцидентов информационной безопасности очень важно своевременное реагирование на них. Поэтому для SIEM-системы большое значение имеет ее вычислительная мощность – скорость выполнения определенных операций, среди которых обработка правил корреляции, хранение данных (чтение/запись) и прочие.

Визуализация собираемых данных

Фактором, который может препятствовать анализу событий безопасности, является отсутствие понятного и достоверного средства визуализации данных. Специалистам кибербезопасности важно наличие поддержки современных инструментов визуализации, поскольку именно на основе отображаемых данных сотрудники оценивают текущую обстановку и выбирают необходимый способ реагирования.

Масштабируемость

Для улучшения процессов реагирования требуется больше мощностей за счет увеличения количества устройств и систем, охваченных SIEM. При масштабируемости SIEM-система может расширяться не только за счет увеличения аппаратного обеспечения, но и с точки зрения обрабатываемых событий безопасности.

Хранение

Исторические данные необходимы не только для обеспечения соответствия нормативным требованиям и предоставления доказательной базы для проведения расследований. Этими данными также пользуется технология UEBA для осуществления глубокого поведенческого анализа[8]. Поэтому SIEM-системе важно использовать распределенные хранилища данных для долгосрочного хранения обработанных событий.

Таким образом, SIEM-системе, чтобы реагировать на инциденты безопасности как можно раньше, необходимо совмещать в себе все вышеперечисленные функциональные возможности на высоком уровне их реализации.

[8] Что такое UEBA? URL: https://encyclopedia.kaspersky.ru/glossary/ueba/ (дата обращения: 27.09.2023)

Как работает SIEM-система

Теперь, когда мы рассмотрели основные функциональные качества системы, поговорим про этапы работы.

Среди основных этапов:

1. Собирает/получает и консолидирует логи из различных источников. К ним относятся: серверы, рабочие станции, средства защиты информации, межсетевые экраны и прочее. В данном случае SIEM-система работает как агрегатор данных.
2. Фильтрует полученные логи[9] и преобразует их в единый формат. Нормализация необходима для того, чтобы в дальнейшем система могла осуществлять с данными событий различные действия.
3. Выявляет закономерности в событиях (коррелирует) и анализирует логи. Исходя из обработанных данных, система выявляет аномалии, угрозы и атаки, затем формирует инциденты информационной безопасности.
4. Завершающее и немаловажное действие SIEM-системы – это автоматическое и незамедлительное оповещение специалистов кибербезопасности об инцидентах.

По такому принципу работают все SIEM-системы. Тем самым этот инструмент помогает специалистам кибербезопасности выявлять потенциальные и реальные уязвимости и угрозы, которые отдельные системы защиты обнаружить самостоятельно не могут.

SIEM на страже персональных данных

Для соблюдения установленных Правительством РФ требований[10] к защите персональных данных, компаниям необходимо регистрировать события безопасности. Меры по регистрации таких событий должны обеспечивать сбор, запись, хранение информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях. Таким образом, SIEM-система – это продвинутое и гибкое решение для исполнения мер обеспечения безопасности персональных данных.

Для большей защиты персональных данных и иной конфиденциальной информации SIEM интегрируется с такими средствами обеспечения безопасности как DLP-системы[11] и антивирусное программное обеспечение, сокращая тем самым риск утечки информации.

> Утечки персональных данных не происходят внезапно. Это ряд событий, которые сотрудники информационной безопасности упустили из вида и/или в отношении которых не были вовремя приняты необходимые контрмеры.

Симбиоз SIEM и DLP позволяет повысить оперативность реагирования на инциденты, ведущие к утечке персональных данных, благодаря получению полной информации о действиях внутреннего нарушителя. Данная интеграция предотвращает различные несанкционированные действия с персональными данными: копирование с компьютеров работников на съемные носители или в облачные хранилища, передачу по электронной почте, а также по другим каналам взаимодействия с третьими лицами. При использовании внутреннего контроля над действиями пользователей и фильтрацией передаваемых данных вероятность раскрытия конфиденциальной информации практически сводится к нулю.

Антивирусное программное обеспечение – один из наиболее распространенных инструментов для защиты персональных компьютеров от атак с использованием вредоносных программ. Интеграция SIEM и антивируса позволяет выявлять активные заражения, способствующие утечке персональных данных. Все данные о срабатываниях антивируса, установленного на всех рабочих станциях компании, серверах, включая почтовые, передаются в SIEM, где сотрудники могут определить исходное событие, которое способствовало заражению устройства. Проанализировав журналы регистрации событий, специалисты кибербезопасности могут предотвратить дальнейшее распространение такого заражения на других персональных компьютерах. Такая совместная работа дает возможность оперативно локализовать инцидент, тем самым предотвратить возможную утечку персональных данных.

[9] Под «логами» можно понимать файл с информацией о действиях программного обеспечения или пользователей.

[10] Пункт 1 Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Справочная правовая система «КонсультантПлюс».

[11] Подробнее про DLP-системы (англ. Data Leak Prevention) читайте во втором выпуске Sber Privacy Journal. URL: http://www.sberbank.ru/common/img/uploaded/kibrary/dpo/sber_privacy_journal_2_2022.pdf (дата обращения: 27.09.2023).

Заключение

Итак, какую же роль SIEM-система играет для обеспечения безопасности персональных данных?

Во-первых, функционирование крупных компаний подразумевает наличие непрерывных потоков большого количества персональных данных и иной конфиденциальной информации, которые необходимо обрабатывать. SIEM является комплексным решением для обеспечения безопасности информации, которое помогает специалистам кибербезопасности выявлять потенциальные угрозы до того, как они приведут к утечке и/или нанесут значительный ущерб бизнесу и причинят вред субъекту персональных данных.

Во-вторых, функциональные качества SIEM позволяют компании получить необходимые метаданные по фактам компьютерного инцидента, в том числе с персональными данными. С учетом того, что для операторов персональных данных законодательно закреплена обязанность в случае установления факта утечки персональных данных своевременно направить уведомление в Роскомнадзор[12], а также предоставить сведения о персональных данных, подвергнутых утечке, и о результатах внутреннего расследования, такие возможности SIEM являются ее большим преимуществом.

В-третьих, благодаря, в том числе, использованию такого комплексного решения как SIEM, клиентские данные находятся под надежной защитой. Во многом поэтому это решение используется SOC[13] СберБанка, эксперты которого круглосуточно обеспечивают информационную безопасность, предотвращают атаки на информационные системы, своевременно реагируют на них и восстанавливают информационные системы в случае реализации атак. По этой же причине данное решение используется коммерческими центрами кибербезопасности, представляющими собой совокупность специалистов, процессов и технологий, которые привлекаются небольшими компаниями для обеспечения информационной безопасности.

Несмотря на все преимущества использования такого инструмента предотвращения утечек персональных данных как SIEM, важно понимать, что для выполнения требований по защите персональных данных, он может оказаться практически бесполезным, если собираемые данные об инцидентах не будут обрабатываться надлежащим образом и использоваться для оптимизации существующих и формирования новых правил корреляции, направленных на выявление и нейтрализацию угроз безопасности персональных данных.

автор
Вера Лебедева

[12] Часть 3.1 статьи 21 Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ // Справочная правовая система «КонсультантПлюс».

[13] SOC СберБанка. URL: https://www.sberbank.ru/soc (дата обращения: 27.09.2023).

Terra incognita

Что такое обезличенные данные и как с ними нужно работать

Обезличивание персональных данных.
Как его нужно проводить?
Что можно делать с обезличенными данными?
Являются ли обезличенные данные персональными?
Как передавать и хранить обезличенные данные?

Этими вопросами рано или поздно задается каждый, кто работает с данными, в том числе с персональными, выстраивает бизнес-процессы, обеспечивает правовое сопровождение бизнеса или отвечает за защиту конфиденциальной информации. Если опытный специалист в сфере приватности сразу скажет, что с вопросами по обезличиванию персональных данных не все так просто, то представители бизнес-подразделений или ИТ-специалисты порой видят в обезличенных данных спасение от всех «бед»: им кажется, что не надо брать согласие на передачу таких персональных данных третьим лицам, не нужно обеспечивать конфиденциальность при их передаче, их можно обрабатывать в любых целях и сколь угодно долго. При этом нельзя сказать, что они однозначно не правы.

Рассмотрим более подробно этот вид данных с точки зрения его природы, применимого законодательства и практики использования, чтобы ответить на наши вопросы.

Откуда появился термин

С точки зрения толкования, с которым мы можем ознакомиться в Большом толковом словаре русского языка[1], термин «обезличивание» означает «лишение отличительных черт, индивидуальных особенностей, присущих каждой отдельной личности, сделать похожим на других; лишить самостоятельности, возможности проявления себя как личности»[2].

Однако в связи с тем, что институт приватности, в том виде, в котором мы его знаем, возник относительно недавно[3], прежде, чем приступить к подробному изучению термина «обезличивание», который используется в отношении обработки персональных данных в современной практике, давайте рассмотрим, как и в каком смысле использовался этот термин до появления первого международного соглашения, направленного на обеспечение права физических лиц на неприкосновенность их частной жизни в отношении автоматизированной обработки персональных данных.

Так, в социологии и философии широко используется словосочетание «обезличенный человек», означающее отказ человека от эмоций, желаний и себя как творческой личности. Понятие «обезличенный человек» было впервые использовано немецким философом Гансом Йонасом в работе «Организм и свобода», опубликованной в 1973 году. Под этим термином Йонас понимал тенденцию современного общества к стремлению ко все большей анонимности человека, лишению его своего собственного, личного, уникального бытия и превращению в одного из множества однотипных организмов. Указанное было связано с массовой индустриализацией и, на первый взгляд, никак не относится к теме обезличивания персональных данных. Однако, при более глубоком рассмотрении, в обоих случаях идет речь об «утрате личности». Действительно, с точки зрения морфологии, термин «обезличивание» означает действие, направленное на «лишение лица», становление «безликим», то есть ничем не выделяющимся из общего ряда. Это значит, что фактически обезличивание именно персональных данных является проекцией обезличивания человека на плоскость его данных в цифровом современном мире.

В российском законодательстве основным законом, устанавливающим правила и требования к обработке персональных данных, является Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (далее – 152-ФЗ). К персональным данным, в соответствии с 152-ФЗ, относится ***«любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)»***. Ранее мы уже рассказывали вам в одной из статей журнала[4] о том, какие данные относятся к персональным и как их выделить среди множества данных, с которым вы работаете. Этим же законом определяется понятие «обезличивание персональных данных» как одно из действий, совершаемых при обработке персональных данных – «**действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных»** (п. 9 ст. 3 152-ФЗ).

Рассмотрим подробнее, что значит принадлежность к «конкретному субъекту персональных данных». Используя определение персональных данных из 152-ФЗ, сформулируем определение субъекта персональных данных:

> Субъект персональных данных – это прямо или косвенно определенное или определяемое физическое лицо. Таким образом, обезличиванием являются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных прямо или косвенно определенному или определяемому физическому лицу.

С точки зрения обработки данных это означает, что мы должны провести такое преобразование персональных данных, в результате которого аннулируется возможность прямого или косвенного определения физического лица без использования дополнительной информации. При этом значимым является условие из определения **«без использования дополнительной информации»**, то есть презюмируется, что с использованием такой информации принадлежность персональных данных установить возможно. Именно поэтому обезличенные данные по-прежнему остаются персональными данными.

Итак, перефразируем для лучшего понимания и осмысления: обезличивание – это такая обработка персональных данных, после которой принадлежность данных конкретному субъекту персональных данных можно установить только с использованием дополнительной информации. При этом данные, полученные в результате обезличивания, являются персональными данными.

[1] С.А. Кузнецов. Большой толковый словарь русского языка. Санкт-Петербург: Норинт, 1998. 1534 с.

[2] Определение глагола «обезличить» – несовершенный вид глагола «обезличивать», от которого образован термин «обезличивание».

[3] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (заключена в г. Страсбурге 28.01.1981) // Справочная правовая система «КонсультантПлюс».

[4] Сердечнюк Е.В., Беляев О.Г. AB OVO: отнесение информации к персональным данным и их классификация // Sber Privacy Journal. 2022. № 2. 2022. С 8-10.

Важно отметить: для осуществления обезличивания организация должна иметь высокий уровень зрелости описания данных, который заключается в следующем: приоритете структурированных данных над слабо или вообще не структурированными, идентификации информационных активов организации и атрибутов данных и использовании организацией единых (однотипных) прямых и косвенных идентификаторов в каждом информационном активе (схеме, таблице, базе данных), что позволяет работать с заголовками таблиц данных и исключает некачественное обезличивание по причинам семантической неоднородности[5].

[5] Семантическая неоднородность – различия в значении, интерпретации и предполагаемом использовании одних и тех же или связанных данных в различных схемах или наборах данных одного домена или внутри одной организации.

Познакомимся с примером обезличивания. Рассмотрим задачу по осуществлению аналитики покупок физических лиц – клиентов банка. Для проведения такой аналитики необходим реестр финансовых транзакций:

ФИО
Номер банковской карты
Номер расчетного счета
Сумма транзакции MMC[6]
код продавца

С целью минимизации обрабатываемых данных в ходе решения задачи, не касаясь вопросов обеспечения оснований для обработки персональных данных и полномочий доступа у исполнителя, проведем процедуру обезличивания реестра:

1. для начала создадим таблицу, где каждому клиенту по ФИО присвоим уникальный ID;
2. затем удалим данные о номерах банковских карт и номерах расчетных счетов;
3. заменим ФИО клиентов на присвоенные им ID.

Так, реестр, изначально содержавший прямые и косвенные идентификаторы персональных данных, стал содержать только информацию о сумме покупки и MMC коде продавца, причем каждая такая операция привязана к конкретному ID:

ID
Сумма транзакции
MMC код продавца

Это и есть обезличенные данные, которые без дополнительной информации (в виде таблицы замен) нельзя отнести к конкретному физическому лицу. Как мы видим, в данном примере обезличенные персональные данные были получены путем замены атрибутов на ID и удаления нескольких атрибутов. Закономерен вопрос: какие еще есть способы обезличивания?

Ответ на него можно получить из нормативных актов и разъяснений[7] Роскомнадзора – уполномоченного органа по защите прав субъектов персональных данных в Российской Федерации (далее – РФ). Формально Приказ № 996 применим только для государственных или муниципальных органов, однако на практике может учитываться коммерческими организациями в качестве лучшей практики и, кроме того, позволяет нам познакомиться с существующими типовыми методами обезличивания.

[6] Четырехзначный номер, классифицирующий вид деятельности торговой точки в операции оплаты по банковским картам.

[7] Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (далее – Приказ № 996); Методические рекомендации по применению приказа Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

Обезличивание по закону

В соответствии с Приказом № 996, обезличивание персональных данных должно обеспечивать не только конфиденциальность, но и возможность обработки таких данных для достижения поставленных задач. Ведь можно удалить все прямые и косвенные идентификаторы персональных данных, но что потом делать с оставшимися атрибутами? Чтобы обезличенные данные были полезны, они должны обладать свойствами, сохраняющими основные характеристики исходных персональных данных. Для оптимального управления балансом уровня обезличивания и возможностью извлекать из обезличенных данных выгоду вводятся свойства обезличенных данных и свойства методов обезличивания:

Свойства обезличенных данных

- полнота;
- структурированность;
- релевантность;
- семантическая целостность;
- применимость;
- анонимность.

Свойства методов обезличивания

- обратимость;
- вариативность;
- изменяемость;
- стойкость;
- возможность косвенного деобезличивания;
- совместимость;
- параметрический объем;
- возможность оценки качества данных.

Среди различных методов следует выбирать такие, которые обеспечивают необходимые свойства обезличенных данных, удовлетворяют потребностям заказчика с точки зрения стойкости, возможности косвенного деобезличивания[8] и прочим требуемым свойствам и, что немаловажно, реализуемы на практике в различных программных средах, а также позволяют решить поставленные задачи. К наиболее перспективным и удобным в практическом применении относятся следующие типовые методы:

- метод введения идентификаторов;
- метод изменения состава или семантики;
- метод декомпозиции;
- метод перемешивания.

При выборе метода обезличивания необходимо руководствоваться целями обработки персональных данных. Следует помнить, что одни и те же методы обезличивания, используемые на различных наборах данных, могут давать разный успех обезличивания. Для достижения наилучшего результата обезличивания или увеличения ценности обезличенных данных возможно объединение различных методов в одну процедуру. При выборе метода и процедуры обезличивания советуем учитывать:

- объем персональных данных (некоторые методы неэффективны на малых объемах);
- область обработки (необходим ли доступ третьим лицам или объединение с данными третьих лиц);
- способы хранения;
- частоту внесения изменений в данные и их количество;
- типы задач обработки.

[8] Под деобезличиванием понимается процедура, обратная обезличиванию, когда обезличенные данные обогащаются дополнительной информацией таким образом, что результирующий набор данных больше не является обезличенным.

Так, целесообразно[9] применять следующие методы:

[9] Ниже приводятся примеры сценариев, когда конкретные методы, как представляется, наиболее эффективны.

Предположим, что мы приняли во внимание все критерии, проанализировали набор данных, подлежащий обезличиванию, выбрали метод обезличивания и реализовали его. На первый взгляд может показаться, что требования к работе с обезличенными данными отсутствуют и от нас не требуется обеспечение безопасности и осмотрительности при работе с такими данными, но это не так. При работе с обезличенными персональными данными необходимо обеспечивать:

- Раздельное хранение обезличенных персональных данных и дополнительной информации о выбранном методе и параметрах процедуры обезличивания.
- Конфиденциальность дополнительной информации о выбранном методе и параметрах процедуры обезличивания.
- Конфиденциальность канала передачи обезличенных персональных данных совместно с информацией о выбранном методе и параметрах процедуры обезличивания.
- Наличие правовых оснований для обработки (ч. 1 ст. 6 152-ФЗ) и соблюдение иных требований законодательства о персональных данных как для обезличенных, так и деобезличенных данных.
- Все требования по безопасности получаемых при деобезличивании данных.

Так почему же нужно защищать обезличенные персональные данные? Для ответа на этот вопрос рассмотрим актуальные угрозы безопасности обезличенных персональных данных. Напомним, что под актуальными понимаются угрозы, реализация (возникновение) которых может привести к нарушению безопасности персональных данных, а именно к нарушению конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности или достоверности[10].

Определяя негативные последствия, которые могут наступить от реализации угроз безопасности обезличенных персональных данных, будем считать угрозу косвенного деобезличивания неактуальной[11]. Так, для субъекта персональных данных остаются релевантными такие негативные последствия, как угроза жизни, здоровью, финансовый и иной материальный вред, модификация персональных данных и нарушение иных прав и свобод. Указанные последствия могут наступить в связи с несанкционированным уничтожением, изменением или блокированием обезличенных персональных данных. При этом, в случае актуальности угрозы косвенного деобезличивания, сохраняется также необходимость в обеспечении конфиденциальности обезличенных персональных данных.

[10] Методический документ. Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021) // Справочная правовая система «КонсультантПлюс».

[11] Тем не менее надо учитывать, что в зависимости от метода и параметров обезличивания актуальность угрозы может сохраняться.

Не углубляясь в конкретные актуальные угрозы, можно однозначно сказать, что для обезличенных персональных данных актуальны как минимум **угрозы безопасности персональных данных 3-го типа**[12], не связанные с наличием недекларированных возможностей в системном и прикладном программном обеспечении, что, в свою очередь, приводит к необходимости обеспечения безопасности обезличенных персональных данных не менее чем для **4-го уровня защищенности** персональных данных, определяемого в соответствии с ПП № 1119.

Таким образом, мы убедились, что в отношении обезличенных персональных данных также необходимо обеспечивать правовые, организационные и технические меры защиты в соответствии с 152-ФЗ. Но, если все так, остается вопрос: зачем нужно обезличивание?

Давайте рассмотрим примеры использования:

1. Работа аналитических и статистических систем, проведение аналитики (этот пример подробно рассмотрен в начале статьи).
2. Передача конфиденциальной информации третьим лицам в агрегированном виде[13] (например, информация о доходах и расходах клиентов по группам возрастов и наличие не менее 100 записей в каждой группе).
3. Работа специалистов по data science и аналитиков данных, возможность удаленной работы (работники могут выполнять функции по анализу данных, выявлению зависимостей между данными и строить гипотезы на данных, не зная какому конкретному человеку данные принадлежат).
4. Работа в среде (разработка, отладка, тестирование программного обеспечения), в том числе подготовка и настройка сред разработки и тестирования (возможность разработки и тестирования функционала приложений на данных, основанных на реальных).
5. Перевод иностранных документов (физическое отсутствие конфиденциальных данных у переводчиков).
6. Разметка данных с целью развития искусственного интеллекта (разделение конфиденциальных данных на множество элементов, не имеющих значимости в отдельности, для ручного анализа и разметки исполнителями).
7. Обмен данными с партнерами при отсутствии необходимости в передаче необезличенных персональных данных (возможность использования незащищенных каналов связи в случае неактуальности соответствующей угрозы безопасности персональных данных).

Анонимизация. Является ли анонимизация синонимом обезличивания?

В РФ термин «анонимизация» не определен ни в 152-ФЗ, ни в иных правовых актах. Однако в отечественных нормативных правовых актах есть предпосылки к введению данного термина.

Так в Приказе № 996, как мы видели ранее, у обезличенных данных есть свойство «анонимность» – ***это невозможность однозначной идентификации субъектов данных, полученных в результате обезличивания, без применения дополнительной информации***[14]. Данный термин также упоминается в ГОСТ 29100[15] в следующей формулировке: анонимность – ***свойство информации, не позволяющее прямо или косвенно определить субъекта персональных данных***.

Учитывая оба определения, сформулируем термин «анонимизация персональных данных» по аналогии с обезличиванием: ***анонимизация персональных данных – действия, в результате которых становится невозможным даже с использованием дополнительной информации прямо или косвенно определить принадлежность данных конкретному субъекту персональных данных***.

Используя определение субъекта персональных, которое мы вывели в начале статьи, можем также сформулировать необходимое условие для анонимизации: невозможность отнесения данных ни к прямо, ни к косвенно определенному или определяемому физическому лицу.

[12] Согласно Постановлению Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – ПП № 1119).

[13] Важно отметить, что при консервативном толковании 152-ФЗ обезличивание персональных данных не может являться самостоятельным основанием для передачи данных третьим лицам. Для осуществления передачи в рамках такого подхода необходимо обеспечить правовые основания для передачи и наличие договора с контрагентом.

[14] Методические рекомендации по применению приказа Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

[15] Межгосударственный стандарт «ГОСТ ИСО/МЭК 29100-2021 Основы защиты персональных данных».

Для того, чтобы оценить корректность введенного термина, рассмотрим практику иностранного законодательства, например, GDPR[16], как наиболее всеобъемлющего регламента в области приватности. GDPR оперирует терминами «псевдонимизация»[17] и «анонимизация». И если по определению псевдонимизация практически полностью соответствует обезличиванию по смыслу 152-ФЗ, то явного определения термина «анонимизация» в GDPR нет. Так, в преамбуле 26 указывается на отсутствие необходимости в применении принципов защиты персональных данных к «анонимной информации, которая не относится к идентифицированному или к поддающемуся идентификации физическому лицу, а также… к персональным данным, анонимизированным таким образом, что субъектов данных вообще или более невозможно определить». Схожесть в значении термина явно прослеживается, однако отсутствие в РФ законодательно установленных правил, критериев и методик не позволяет в полном объеме использовать возможности анонимизации, оставляя серую зону в практике ее применения.

Аналоги обезличивания/анонимизации

В завершение хотелось бы отметить, что обезличивание и анонимизация – это не единственные методы преобразования данных с целью сокрытия личности владельца. Некоторые из иных подходов вы уже могли встречать:

- **Токенизация**[18] – процесс замены конфиденциального элемента данных на неконфиденциальный эквивалент (токен), который не имеет самостоятельного смысла/значения для внешнего или внутреннего использования.
- **Маскирование (обфускация)**[19] – способ защиты конфиденциальной информации от несанкционированного доступа путем замены исходных данных фиктивными или произвольными символами. При этом замаскированная информация выглядит реалистично и непротиворечиво и может использоваться в процессе тестирования программного обеспечения.
- **Гомоморфное шифрование**[20] – форма шифрования, которая позволяет выполнять вычисления с зашифрованными данными без их предварительного дешифрования. Результирующие вычисления остаются в зашифрованном виде, который при расшифровке приводит к идентичному результату, полученному при выполнении операций с незашифрованными данными.

Заключение

Подводя итог подчеркнем, что несмотря на наличие требований к осуществлению обезличивания и последующей обработки обезличенных персональных данных таким образом, чтобы не причинить вреда субъекту персональных данных, обезличивание является широко распространенным способом снижения рисков несанкционированного разглашения персональных данных при их обработке в автоматизированной системе. Также обезличивание применяется при передаче данных между системами или между контрагентами, в том числе путем ограничения количества работников, которые имеют доступ к необезличенным данным, без потери бизнес-выгоды. Анонимизация же позволяет полностью нивелировать такое свойство данных как конфиденциальность. Однако для этого требуется законодательное закрепление понятия анонимизация и критериев анонимизированных данных, на скорейшую реализацию которого и будем надеяться.

автор
Олег Беляев

[16] Регламент № 2016/679 Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)» (GDPR).

[17] «Псевдонимизация» – это обработка персональных данных таким образом, что их больше невозможно отнести к конкретному субъекту данных без использования дополнительной информации, при условии, что такая дополнительная информация хранится отдельно, и в отношении нее приняты технические и организационные меры, предотвращающие ее отнесение к идентифицированному или идентифицируемому физическому лицу (согласно GDPR).

[18] Пример использования: токенизация данных платежных карт.

[19] Пример использования: функциональное/нагрузочное тестирование.

[20] Пример использования: электронное голосование.

Коммерческая биометрия в России

Конец или новое начало?

Использование биометрических технологий в правоохранительной, а затем и в коммерческой сферах исторически определялось, в первую очередь, достижениями науки, которые давали возможность путем измерения биологических и физиологических особенностей человека проводить его однозначную идентификацию. В разное время роль основного биометрического параметра, применявшегося в системе идентификации, играли различные характеристики тела человека: от антропометрии до ДНК.

Значимые события развития биометрии

1879 Альфонс Бертильон (Франция) изобрел систему «бертильонаж» для идентификации преступников по их антропометрическим данным (измерение тела человека и его частей).

1892 Фрэнсис Гальтон (Великобритания) доказал уникальность отпечатков пальцев, что позволило идентифицировать человека.

1965 Вудро Бледсоу, Хелен Чан Вольф и Чарльз Бисон (США) создали первоначальную технологию распознавания лиц в рамках коллективного исследования.

1974 В США появились первые коммерческие системы идентификации по геометрии руки в целях контроля физического доступа.

1970-80 В Италии создана и адаптирована первая система идентификации по голосу.

1994 Джон Дафман запатентовал алгоритм для обнаружения различий на сетчатке глаза человека.

1996 Внедрена систем доступа по ладони на Олимпийских играх в Атланте в рамках контроля и защиты физического доступа к Олимпийской деревне.

1998 ФБР запущена криминалистическая система цифрового хранения и поиска ДНК-маркеров для правоохранительных органов CODIS.

2001 11 сентября произошла серия террористических актов на Всемирный торговый центр, которая значительно повысила интерес к технологиям биометрической идентификации. В первую очередь это коснулось транспортных систем, обеспечивающих международное перемещение людей.

2005 188 государств-членов Международной организации гражданской авиации (ИКАО) утвердили стандарт, согласно которому начали выдавать машиносчитываемые паспорта.

2013 Компания Apple внедрила в свои смартфоны функцию распознавания отпечатков пальцев – Touch ID.

2017 Apple внедрила в смартфоны функцию распознавания лица – Face ID.

2020 Скачок внедрения тепловизионного контроля и отслеживания контактов с инфицированными в сочетании с бесконтактной биометрией в условиях пандемии COVID-19.

До недавнего времени вопрос регулирования использования биометрических технологий в России покрывался, по сути, только Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ (далее – 152-ФЗ), согласно которому под биометрическими персональными данными понимаются:

> «Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных».

В связи с реализацией государственной политики в части повышения безопасности обработки биометрических персональных данных, в конце 2022 года вступил в силу Федеральный закон от 29.12.2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» (далее – 572-ФЗ).

Закон полностью исключает хранение биометрических персональных данных в целях идентификации и аутентификации физических лиц как государственными, так и коммерческими организациями. В настоящей статье рассмотрим основные особенности применения нового закона, а также изменения, которые коснулись операторов и субъектов биометрических персональных данных.

Внедрение Единой биометрической системы в России

Работа над созданием Единой биометрической системы (ЕБС) началась еще в 2017 году по инициативе Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) и Центрального Банка Российской Федерации (ЦБ РФ). Разработчиком системы являлся Ростелеком. В настоящее время Постановлением Правительства РФ от 16.12.2022 №2326[1] функции оператора ГИС «Единая биометрическая система» возлагаются на АО «Центр биометрических технологий» (ЦБТ), созданное в соответствии с указом Президента РФ № 693 от 30.09.2022.

Также в декабре 2017 года был принят закон[2], позволяющий кредитным организациям открывать счета (вклады) клиентам (физическим лицам) предоставлять им кредиты, осуществлять переводы денежных средств по таким счетам без их личного присутствия. Достоверность сведений о таких клиентах – удаленная идентификация – подтверждалась совместным применением Единой системы идентификации и аутентификации (ЕСИА), а также ЕБС[3]. Согласно требованиям вступившего в силу закона планировалось, что к 1 января 2019 года к ЕБС будут подключены 20% банковских отделений, к 1 июля 2019 года – 60%, и, наконец, к 1 января 2020 года к ЕБС будут подключены все отделения банков на территории России.

Полностью ЕБС была внедрена 30 июня 2018 года. Список кредитных организаций, уполномоченных собирать биометрическую информацию и предоставлять дистанционные услуги с использованием удаленной идентификации, на тот момент насчитывал 438 банков. Обретшая жизнь удаленная идентификация позволяла гражданам получать финансовые услуги дистанционно в любом банке. Для этого необходимо было один раз пройти первичную идентификацию в кредитной организации, уполномоченной на сбор биометрических персональных данных в ЕБС, где сотрудник банка:

- в присутствии физического лица проверял его паспорт и СНИЛС;
- при отсутствии аккаунта обратившегося клиента регистрировал его в ЕСИА;
- а также снимал необходимые биометрические данные – изображение лица и текстозависимую запись голоса.

Далее для дистанционного открытия счета (вклада), получения кредита или осуществления перевода в новом для себя банке гражданину необходимо было пройти авторизацию в ЕСИА и подтвердить свои биометрические данные с помощью смартфона, планшета или компьютера с использованием камеры и микрофона этих устройств.

Банки, в свою очередь, могли подключаться к ЕБС в одной из следующих ролей:

- поставщика биометрических данных, то есть в роли организации, которая регистрирует биометрические данные граждан;
- потребителя сервиса удаленной идентификации, то есть организации, которая получает результат удаленной идентификации – персональные данные клиентов с использованием ЕСИА и ЕБС;
- организации, единовременно выполняющей роль поставщика биометрических данных и потребителя сервиса удаленной идентификации.

Однако внедрение точек сбора биометрии оказалось довольно затруднительным для небольших банков ввиду высоких расходов на реализацию требований защиты информации при подключении к ЕБС. Во многом поэтому темпы внедрения ЕБС были снижены, и в конце 2020 года соответствующим федеральным законом[4] были внесены изменения, касающиеся сбора и использования биометрических персональных данных. Так, ЕБС разрешили применять не только для открытия счета и выдачи кредита физическим или юридическим лицам, но и для любых финансовых услуг. Для небольших банков (банков с базовой лицензией) сбор биометрии в ЕБС стал не обязанностью, а правом.

[1] Постановление Правительства РФ от 16.12.2022 № 2326 «О возложении на акционерное общество «Центр Биометрических Технологий» функций оператора единой информационной системы персональных данных...» // Справочная правовая система «КонсультантПлюс».

[2] Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации» от 31.12.2017 г. № 482-ФЗ // Справочная правовая система «КонсультантПлюс».

[3] Соответствующие изменения были внесены в ст. 8 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (в настоящее время положения статьи утратили силу ввиду выхода 572-ФЗ).

[4] Федеральный закон от 29.12.2020 г. № 479-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // Справочная правовая система «КонсультантПлюс».

Новые требования к биометрической идентификации и аутентификации

Структура нормативных правовых актов, регулирующих обработку биометрических персональных данных в целях идентификации и аутентификации (по состоянию на сентябрь 2023 г.):

Создание

- Единая биометрическая система
- ФЗ от 29.12.2022 № 572-ФЗ
- ПП РФ от 28.11.2011 № 977
- ПП РФ от 31.05.2022 № 883 положение о ЕБС
- ПП РФ от 16.12.2022 № 2326 об операторе ЕБС
- ПП РФ от 15.06.2022 № 1067 случаи и сроки использования биометрических персональных данных (далее – бПДн)

Согласие

- ПП РФ от 17.03.2023 № 405 правила получения
- ПП РФ от 27.03.2023 № 478 порядок отказа, отзыва
- ПП РФ от 15.10.2021 № 1754 проверка ЭП
- РП от 30.06.2018 № 1322-р форма

Установление личности

- ПП РФ от 28.12.2018 № 1703 порядок предоставления бПДн в МВД
- Приказ Минюста от 30.09.2020 № 228 порядок установления личности
- ГОСТ Р ИСО/МЭК 19794-5-2013
  Информационные технологии. БИОМЕТРИЯ. Форматы обмена биометрическими данными. Часть 5 «Данные изображения лица»

Эксплуатация

Требования

- ПП РФ от 30.06.2018 № 772 к составу и виду бПДн в ЕБС
- ПП РФ от 14.07.2018 № 820 к идентификации
- ПП РФ от 24.03.2023 № 451 к проверке бПДн
- ПП РФ от 15.06.2022 № 1066 к размещению через мобильное устройство
- ПП РФ от 23.10.2021 № 1815 использование бПДн (кроме финансового сектора)
- Приказ Минцифры России от 12.05.2023 № 453 о порядке сбора и обработки бПДн
- Приказ Минцифры России от 17.04.2023 № 378 методика проверки бПДн
- Приказ Минцифры России от 09.09.2022 № 658 регламент размещения бПДн для МФЦ

Плата

- Приказ Минцифры России от 31.03.2023 № 334 Методика расчета взимания платы
- Приказ Минцифры России от 29.06.2021 № 662 максимальный размер платы
- ПП РФ от 22.05.2023 № 810 по порядку аккредитации организаций

Контроль

- ПП РФ от 11.04.2023 № 585 порядок федерального госконтроля (надзора)
- Приказ Минцифры России от 25.02.2022 № 142 проверки аккредитованных лиц
- Указание ЦБ РФ от 21.09.2021 № 5936-У контроль со стороны ЦБ
- Информационное письмо ЦБ РФ от 28.06.2018 г. №ИН-03-13/40 воздержание от санкций за невыполнение

Безопасность

Требования

- ПП РФ от 06.07.2008 № 512 к носителям бПДн
- ПП РФ от 29.06.2018 № 747 к фиксированию действий
- ПП от 15.10.2021 № 1753 для МФЦ
- Приказ Минцифры России от 12.05.2023 № 453 к ИТ и СЗИ
- Приказ Минцифры России от 07.07.2021 № 685 к формам подтверждения соответствия

Контроль

- ПП РФ от 24.03.2023 № 451 со стороны ФСБ и ФСТЭК

Угрозы

- Приказ Минцифры России от 05.05.2023 № 446 актуальные для организаций, использующих бПДн (кроме ЕБС)
- Приказ Минцифры России от 05.05.2023 № 445 актуальные для организаций, использующих бПДн (кроме организаций финансового рынка)
- Приказ Минцифры от 26.11.2020 № 624 актуальные для УЦ
- Указание ЦБ РФ от 16.12.2021 № 6017-У актуальные для кредитных и некредитных организаций
- Указание ЦБ РФ от 16.12.2021 № 6018-У актуальные для организаций финансового рынка
- Методические рекомендации ЦБ РФ от 14.02.2019 № 4-МР по нейтрализации актуальных угроз

Вступивший в силу 572-ФЗ регулирует не столько обработку биометрических персональных данных, сколько процедуры идентификации и аутентификации физических лиц с использованием биометрии в ЕБС. При этом в документе прямо утверждается, что все организации[5] всех форм собственности при работе с биометрическими персональными данными и векторами ЕБС с 1 июня 2023 г. должны осуществлять свою деятельность в соответствии со 152-ФЗ и 572-ФЗ.

Важно отметить, что действие 572-ФЗ **не распространяется** на обработку биометрических персональных данных при непосредственном участии человека.

Также под исключения попали случаи обработки биометрии в целях обеспечения государственной безопасности, среди которых

- оперативно-розыскная деятельность;
- контрразведывательная деятельность;
- оборона страны;
- обеспечение безопасности государства;
- охрана правопорядка;
- реализация внешней политики;
- обеспечение санитарно-эпидемиологического благополучия;
- а также функционирование государственной системы миграционного и регистрационного учета, изготовления, оформления и контроля документов, удостоверяющих личность.

Регулирование по 572-ФЗ касается, при этом, только изображения лица человека, полученного с помощью фото/видеоустройств и записи голоса человека, полученной с помощью звукозаписывающих устройств. Требований к регулированию иных видов биометрических данных: геометрия контура рук, изображение радужной оболочки глаза, изображение отпечатка пальца и других, – не предъявляется.

Ключевым изменением в порядке обработки биометрических персональных данных (изображения лица и записи голоса) в связи с вступлением в силу 572-ФЗ является прямой запрет на сбор и хранение биометрических персональных данных на стороне организации любой формы собственности, за исключением уполномоченных банков и самой ЕБС. Также для сбора биометрических персональных данных планируется подключить многофункциональные центры и мобильные приложения ЕБС и ее региональных сегментов. Организации, осуществлявшие ранее сбор биометрии в своих целях, обязаны прекратить такой сбор и удалить свои базы биометрических персональных данных, предварительно передав такие базы данных в ЕБС. Дата завершения передачи баз биометрических данных – 30 сентября 2023 года.

Таким образом, при желании клиента организации – физического лица – получить услугу с использованием биометрии при идентификации и аутентификации, ему необходимо пройти процедуру идентификации в ЕБС, дать согласие на обработку такой организацией его биометрических персональных данных и векторов ЕБС через Портал «Госуслуги»[6], а затем уже предъявить свои биометрические персональные данные для аутентификации и последующего получения услуги. Организация при аутентификации осуществит сбор биометрических образцов лица или голоса, но только лишь для того, чтобы передать их в ЕБС для дальнейшей обработки. После оказания услуги данные первичной биометрии могут сохраняться организацией до 10 дней на случай разбора возможных претензий со стороны субъекта.

[5] Согласно п. 7 ст. 3 572-ФЗ под действие закона подпадают следующие организации при использовании ими биометрических персональных данных в целях идентификации и аутентификации: банки, многофункциональные центры предоставления государственных и муниципальных услуг и иные организации, размещающие сведения в единой биометрической системе, государственные органы, органы местного самоуправления, Центральный банк РФ, организации, индивидуальные предприниматели, нотариусы, органы государственной власти субъектов РФ, подведомственные им организации, органы местного самоуправления, подведомственные им организации, иные организации, оператор единой биометрической системы, оператор регионального сегмента единой биометрической системы.

[6] Портал «Госуслуги» – Федеральная государственная информационная система «Единый портал государственных и муниципальных услуг (функций)».

Обработка биометрических персональных данных и предоставление векторов со стороны ЕБС для подключившихся к ЕБС организаций осуществляется на возмездной основе.

Необходимо также отметить, что законом вводится новое понятие – «Вектор единой биометрической системы».

- Под вектором ЕБС в 572-ФЗ понимаются персональные данные, «полученные в результате математического преобразования биометрических персональных данных физического лица, содержащихся в единой биометрической системе, которое произведено с использованием информационных технологий и технических средств», соответствующих требованиям 572-ФЗ.
- Согласно ГОСТ Р 52633.4-2011 «Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия - код доступа» (статья 3.13) «вектор» – это «...нумерованный набор биометрических параметров или производных от них параметров, имеющих одну и ту же интерпретацию и формат представления».

Другими словами, вектор по определенному алгоритму создает из первичной биометрии (биометрического образца) цифровой слепок, позволяющий производить автоматизированное сравнение двух векторов и формировать решение о степени их соответствия. Обратное преобразование из вектора в изображение лица или другой исходный биометрический образец математически не считается возможным. Именно поэтому, во-первых, по вектору без дополнительных сведений невозможно установить субъекта, биометрический образец которого лег в основу формирования вектора, во-вторых, вектор как таковой выведен из регулирования 152-ФЗ.

Векторы

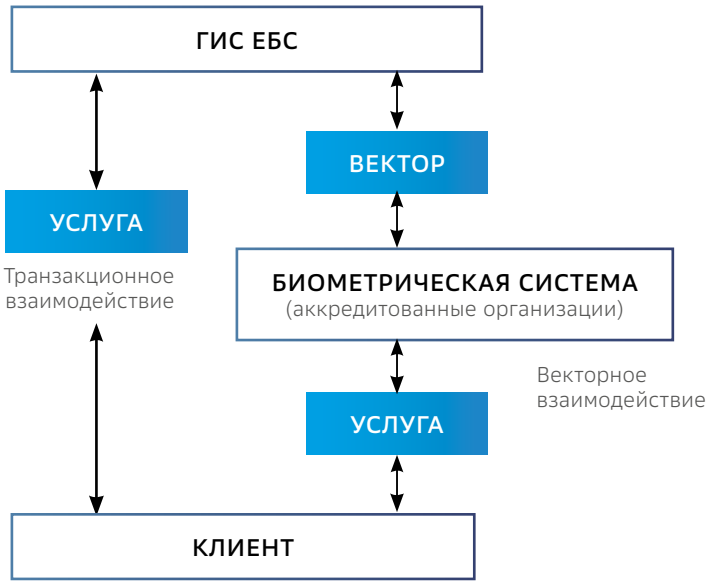
Образцы

Требования к организациям при работе с ЕБС

Доступ к ЕБС получат только уполномоченные и аккредитованные организации. Аккредитация является обязательной, если организация планирует работать с векторами ЕБС на своей стороне, а также оказывать услуги другим компаниям по распространению биометрических технологий.

ЕБС предлагает две модели взаимодействия: векторную и транзакционную. В случае транзакционного взаимодействия организация при получении биометрических персональных данных от клиента в целях оказания ему услуг сразу направляет их в ГИС ЕБС, где уже происходит преобразование биометрии в вектор, сверка полученного вектора с векторами, размещенными в ЕБС, и формирование ответа, который и возвращается организации. При такой схеме взаимодействия скорость обслуживания клиента может значительно снизиться, так как на отправку данных и получение ответа от ГИС ЕБС уходит до 2 минут. При векторном взаимодействии организация, оказывающая услуги посредством биометрических персональных данных, может организовать хранение векторов ЕБС на своей стороне, по сути сформировав свою «коммерческую» биометрическую систему (КБС). Соответственно, такая организация может производить преобразование биометрических персональных данных в вектор, сравнение векторов и формирование ответа о степени совпадения на своей стороне, что способно существенно повысить скорость обслуживания. Обязательным условием подключения к ЕБС по модели векторного взаимодействия является прохождение аккредитации и выполнение требований информационной безопасности.

Схему транзакционного и векторного взаимодействия с ЕБС можно представить следующим образом:



Статус аккредитованной организации после получения аккредитации является бессрочным, но уполномоченный орган[7] оставляет за собой право проводить периодические проверки соответствия организации требованиям аккредитации. Для прохождения аккредитации организация должна подтвердить выполнение следующих требований:

- отсутствие иностранного резидентства;
- объем капитала от 500 миллионов рублей;
- финансовое обеспечение ответственности за убытки третьим лицам, вследствие возможных ошибок аутентификации с использованием биометрических персональных данных, не менее 100 миллионов рублей;
- размещение баз данных векторов ЕБС на территории РФ;
- подключение к ГосСОПКА[8];
- наличие лицензии ФСБ России на виды работ с СКЗИ (в случае, если планируется оказание услуг третьим лицам с использованием СКЗИ);
- законное право собственности на аппаратные и программные СКЗИ;
- не менее двух работников в штате, имеющих высшее образование в сфере информационных технологий;
- подтверждение чистоты деловой репутации единоличного исполнительного органа/членов коллегиального исполнительного органа, учредителей организации[9];
- достоверность сведений об организации, внесенных в ЕГРЮЛ (не должны содержать отметку о недостоверности).

Организация, не желающая проходить аккредитацию, обязана прекратить обработку биометрических персональных данных и векторов или же воспользоваться услугами ГИС ЕБС и/или аккредитованной организации по соответствующему договору.

> Важно отметить, что Приказ Минцифры России от 12.05.2023 г. № 453[10] отменяет прежний порядок обработки биометрических персональных данных. Теперь обработка биометрии и векторов в ЕБС и организациями должна осуществляться с применением информационных технологий и технических средств, получивших подтверждение об их соответствии установленным требованиям.

Подтверждение соответствия осуществляется Минцифры России в течение 60 рабочих дней с даты получения необходимых документов и сведений. Установлены также требования к качеству размещаемых в ЕБС и ее региональных сегментах биометрических образцов персональных данных в зависимости от целей использования (идентификация или аутентификация) и способов их регистрации – личная явка, саморегистрация, передача из других систем.

[7] Федеральный государственный контроль (надзор) в сфере идентификации и/или аутентификации осуществляется уполномоченным Правительством РФ федеральным органом исполнительной власти – Министерством цифрового развития, связи и массовых коммуникаций РФ согласно Постановлению Правительства РФ № 585 от 11.04.2023 г.

[8] ГосСОПКА – государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак, создаваемая в целях предотвращения и устранения последствий компьютерных атак на критическую информационную инфраструктуру РФ.

[9] Не требуется для организаций, в уставном капитале которых доля владения государства более 50%.

[10] Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 12 мая 2023 г. № 453 «О порядке обработки биометрических персональных данных и векторов единой биометрической системы в единой биометрической системе и в информационных системах аккредитованных государственных органов, Центрального банка Российской Федерации в случае прохождения им аккредитации, организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц» // Справочная правовая система «КонсультантПлюс».

Защита биометрических персональных данных

После того, как организация определится со схемой взаимодействия с ЕБС, а, следовательно, с необходимостью или отсутствием необходимости прохождения процедуры аккредитации, она должна обеспечить защиту оконечных устройств и своего серверного сегмента (при наличии) для работы с ЕБС.

Для защиты информации при организации работы с биометрическими персональными данными, векторами ЕБС и непосредственного взаимодействия с ЕБС должны применяться прошедшие оценку соответствия требованиям безопасности информации средства криптографической защиты информации (СКЗИ), позволяющие нейтрализовать угрозы безопасности биометрических персональных данных, определенные в отраслевых моделях угроз. Отраслевые модели угроз при этом разделены на три основные группы:

1. для государственных органов, органов местного самоуправления, Центрального банка РФ, организаций (за исключением организаций финансового рынка), индивидуальных предпринимателей;
2. для организаций финансового рынка;
3. для органов государственной власти субъектов РФ, подведомственных им организаций, органов местного самоуправления, подведомственных им организаций, иных организаций.

Таким образом, помимо мер, необходимых для защиты персональных данных, дополнительные меры защиты биометрических персональных данных и векторов ЕБС включают в себя криптографическую защиту каналов связи, средства разграничения и контроля доступа, средства создания и проверки электронной подписи (ЭП). СКЗИ, используемые для обеспечения безопасности биометрических персональных данных, а также средства ЭП должны обеспечивать уровень криптографической защиты до КС3/КВ[11].

Кроме того, организация вне зависимости от выбранной модели взаимодействия с ЕБС должна обеспечить использование СКЗИ уровня КС1 и выше на мобильных устройствах.

Согласие и добровольность для субъектов персональных данных

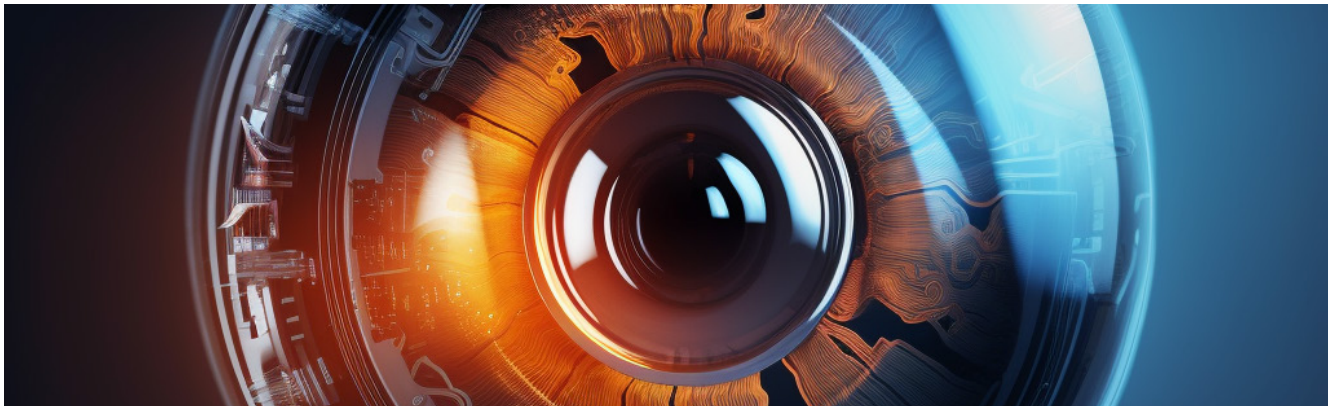
Для субъекта персональных данных обработка биометрии всегда носила строго добровольный характер. Это закреплено в 152-ФЗ и с недавнего времени усилено общим для оператора запретом на отказ от оказания услуг ввиду нежелания субъекта персональных данных предоставлять согласие на обработку его персональных данных (ст. 16 Закона РФ от 07.02.1992 № 2300-1 «О защите прав потребителей»). Вступивший в силу 572-ФЗ еще раз в явном виде утверждает исключительно добровольный характер сдачи биометрических персональных данных физическим лицом, а также запрет отказа в оказании услуг со стороны организаций при нежелании субъекта персональных данных предоставлять согласие на обработку биометрических персональных данных. Кроме того, впервые в законотворческой практике РФ появились такие понятия, как «отказ от обработки биометрических персональных данных» и «отказ от отказа от обработки биометрических персональных данных». Иными словами, субъект биометрических персональных данных может в явном виде запретить обработку своей биометрии, а затем отозвать свой отказ, если по каким-то причинам передумал.

Как было сказано выше, закон обязывает организации до 30.09.2023 передать ранее собранные биометрические персональные данные в ЕБС, при этом уведомив субъекта биометрических персональных данных о такой передаче не позднее, чем за 30 дней до планируемого размещения биометрии в ЕБС. Субъект, в свою очередь, может выразить свой отказ на такую передачу, а значит и на дальнейшее размещение, хранение и использование биометрии в ЕБС. Биометрические персональные данные, не покрытые явным добровольным согласием субъекта, организация обязана удалить.

Приказ Минцифры от 12.05.2023 г. № 453 устанавливает срок хранения биометрических персональных данных в ЕБС. Срок составляет 5 лет. Затем субъекту будет предложено пересдать биометрические образцы, а векторы ЕБС станут недоступны для проведения аутентификации.

> Согласие на обработку биометрических персональных данных может быть дано в одном из отделений уполномоченного на такой сбор банка, Многофункциональном центре предоставления государственных и муниципальных услуг (МФЦ) или же в мобильном приложении ЕБС/регионального сегмента ЕБС как в классической форме (на бумажном носителе), так и в электронной форме (с ЭП).

[11] Встраивание средств криптографической защиты уровня КС3/КВ осуществляется под контролем со стороны ФСБ России.



При этом в согласии на обработку биометрических персональных данных в качестве операторов биометрических персональных данных будут указаны:

- организация, осуществляющая сбор биометрии для оказания услуг;
- оператор ЕБС;
- а также цели обработки биометрии, на которые соглашается субъект.

С 1 января 2024 г. у физического лица появится возможность централизованно управлять своими согласиями на обработку биометрических персональных данных на портале государственных услуг. Сейчас это можно сделать в МФЦ.

Для самого субъекта персональных данных ЕБС предлагает сервисы, многие из которых ранее были доступны только при личном посещении организации физическим лицом. Среди таких сервисов, в частности:

- банковские услуги без физической явки в отделение;
- удаленное заключение услуг связи;
- оформление карты болельщика;
- дистанционная сдача сессии в вузах;
- получение квалифицированной электронной подписи;
- пропуск на территорию правительственных объектов и бизнес-центров;
- иные.

В зависимости от типа ЭП, которая используется для подписания согласия на обработку биометрических персональных данных: усиленная квалифицированная, усиленная неквалифицированная, подтвержденная или не подверженная личной явкой простая, – зависит набор сервисов/услуг, которые может получить субъект биометрических персональных данных. Так, при использовании подтвержденной ЭП субъект может получить до 25 различных услуг, при неподтвержденной – только 4.

Заключение

Из приведенных в статье основных особенностей обновленного законодательства в сфере регулирования обработки биометрических персональных данных в России очевидно, что сбор и хранение данных изображения лица и образцов голоса становится моноцентричным, то есть сосредотачивается в руках одной уполномоченной организации. Представляется, что это позволяет существенно повысить защищенность биометрии, а также полностью исключить бесконтрольную обработку биометрических персональных данных и векторов ЕБС. Персональные данные, однозначно идентифицирующие физическое лицо (ФИО, адрес и прочие), хранятся отдельно от векторов ЕБС и биометрических персональных данных. Таким образом, утечка биометрии и векторов становится бесполезной для злоумышленников. За нарушение требований 572-ФЗ предусмотрена ответственность в виде существенных штрафов, а повторное нарушение грозит запретом на использование биометрии и векторов для организации-нарушителя.

Особое значение имеет пристальное внимание со стороны нового регулирования к соблюдению прав субъекта. Впервые на законодательном уровне проработаны вопросы отказа от обработки персональных данных, а также создан прецедент на уровне государственной системы самостоятельного, централизованного управления своими согласиями на обработку персональных данных субъектом биометрических персональных данных. Также для субъекта предусмотрено больше способов саморегистрации в ЕБС, возможность подписания согласий на сбор и дальнейшую обработку биометрии любым доступным ему видом ЭП, вплоть до простой ЭП, что позволит существенно упростить жизнь граждан.

автор
Татьяна Кузьменко

Риски в онлайн-играх

Как защитить своего ребенка?

Практически каждый из нас знаком с таким современным феноменом как онлайн-игры, однако не многие догадываются, какие риски скрываются за красивой картинкой. В статье вы сможете узнать, к чему может привести бессознательное поведение в онлайн-играх, а также разобраться в способах предотвращения негативных последствий.

Разберемся в понятиях

Онлайн-игры – это веселый и приятный способ времяпрепровождения, способствующий улучшению командного взаимодействия и развитию других навыков. Тем не менее есть несколько рисков, о которых необходимо знать, чтобы помочь детям оставаться в безопасности и получить положительный игровой опыт.

Что такое онлайн-игры?

Онлайн-игра – это видеоигра через интернет, зачастую с другими игроками, находящимися в разных частях света. Это могут быть различные виды игр, включая массовые многопользовательские ролевые онлайн-игры (MMORPG), шутеры от первого лица, стратегии в реальном времени, спортивные симуляторы и другие.

Как работают онлайн-игры?

В онлайн-играх игроки подключаются к серверу или платформе, на которой размещена игра, и могут играть и общаться с другими игроками, также подключенными к ним. Общение в игре возможно с помощью функций чата и голосовой связи, которые позволяют игрокам достигать совместных целей в игре и соревноваться.

На каких устройствах можно играть?

Онлайн-игры можно встретить на игровых консолях – Xbox, PlayStation и Nintendo Switch, на игровых платформах для ПК – Steam, Epic Games и GOG, в магазинах приложений для смартфонов и планшетов – Play и Apple App Store, а также в специально предназначенных для того веб-браузерах (например, Miniclip, Kongregate и Armor Games).

Немного статистики

Согласно статистике CyberSafeKids[1],

детей в сети регулярно играют в онлайн-игры с незнакомцами

не обращают внимание на возрастное ограничение (12+ и выше), которое может скрывать под собой «взрослый контент» (например, нецензурную лексику, сцены насилия и жестокости, слишком откровенные элементы), что может негативным образом сказаться в дальнейшем на детской психике.

При этом в России, по данным исследования Института Современных Медиа[2],

регулярно проводят время за онлайн-играми

Каждый шестой ребенок начинает играть с 2 лет.

Остальные в большинстве случаев – с 5.

Первая платформа – мобильная.

Кроме этого, по данным Лаборатории Касперского, в 2022 году зафиксировано

>5,8 млн случаев обнаружения вредоносных программ и других вирусов, замаскированных под популярные игры, что

на **66%** больше, чем годом ранее[3]

[1] По данным организации CyberSafeKids: https://www.cybersafekids.ie/. CyberSafeKids – благотворительная организация, деятельность которой направлена на расширение возможностей детей, родителей и учителей по безопасному нахождению в сетевом мире.

[2] По данным исследования Института Современных Медиа: https://cyberpsy.ru/articles/children_media_2017_momri/. Институт Современных Медиа – исследовательская компания в области изучения СМИ и бизнес-коммуникаций.

[3] По данным анализа Лаборатории Касперского: https://www.kaspersky.com/about/press-releases/2021_lockdown-gaming-baddies-58-million-attacks-detected-over-the-past-year. Лаборатория Касперского – международная компания, специализирующаяся на разработке систем защиты от компьютерных вирусов, спама, хакерских атак и прочих киберугроз.

Негативный эффект от попадания вируса на устройство может заключаться:

- в повреждении жесткого диска или в замедлении работы устройства и приложений;
- в уничтожении важных файлов;
- а также в хищении личных данных пользователей (в частности, детей).

Таким образом, ребенок в онлайн среде страдает и от негативного воздействия на него самого (поскольку в фокусной зоне находится его персональная информация и, соответственно, безопасность), и от негативного воздействия на устройство.

Риски, связанные с онлайн-играми

Среди самых серьезных рисков, связанных с онлайн-играми, о которых должен знать каждый родитель:

Кибербуллинг[4], преследование и доксинг[5]. Любая многопользовательская игра открывает возможности для преследования. Некоторые игроки могут даже «доксить» других, публикуя в открытом доступе конфиденциальную информацию, фото- или видеоматериалы о них.

Вредоносные программы и вирусы. Загрузка игр с малоизвестных сайтов или открытие файлов, присланных другими игроками, может заразить устройство, с которого ребенок выходит в сеть, опасным вредоносным ПО или другими вирусами: привести к блокированию или сбоям устройства, уничтожению и краже личных данных.

Кража персональных данных. Общение с анонимными игроками в интернете может подвергнуть вашу семью риску кражи личных данных ребенка. Мошенники выдают себя за друзей или других детей, чтобы похитить конфиденциальную информацию о ваших детях или членах семьи и в последующем использовать для получения собственной выгоды, например, для манипуляции вами с целью получить денежные средства.

Фишинговые атаки[6] и захват учетных записей. По статистике компании Kount[7], каждый пятый любитель онлайн-гейминга пострадал от взлома аккаунта за прошедший год. Хакеры атакуют игровые аккаунты детей с помощью фишинговых сообщений или других технических атак, чтобы получить доступ к внутриигровой валюте и подключенным кредитным картам или совершить нападение на других игроков.

[4] Кибербуллинг – вид психологического насилия над человеком, унижение и травля жертвы в социальных сетях и других интернет-ресурсах.

[5] Доксинг – поиск и публикация персональной и/или конфиденциальной информации о человеке без его согласия.

[6] Фишинг – вид интернет-мошенничества, используемый для получения идентификационных данных пользователей.

[7] По данным компании Kount: https://kount.com/blog/21-online-gamers-have-been-hacked-last-year-infographic. Kount – поставщик решений по защите цифровых платформ от внешних угроз.

Онлайновые хищники. В онлайн-играх люди могут стать жертвами киберпреследователей, которые используют безобидную на первый взгляд игровую среду для манипулирования детьми. В некоторых случаях киберпреследование может перерасти в преследование в реальном мире.

Финансовые аферы. Многие игровые сообщества включают в себя развитую внутриигровую экономику, с помощью которой игроки покупают и обменивают цифровые товары на реальные деньги. Киберпреступники используют молодых и неопытных игроков для незаконного заработка.

Зрелый контент. Некоторые известные игровые франшизы известны своим насилием и сексуальными образами. Ряд игровых сообществ, даже созданных для детей, модифицируют существующие игры («моддинг»), делая некоторые элементы в них более откровенными.

Чрезмерное увлечение играми. Дети не всегда обладают достаточной эмоциональной зрелостью, чтобы ограничить время, проведенное за игрой. Поэтому чрезмерное увлечение играми может сказаться на всех сферах жизни – от социального развития до режима сна и успеваемости в школе.

Рекомендации для родителей

Активное участие родителей в онлайн-жизни своих детей позволит не только лучше узнать ребенка и укрепить с ним социальный контакт, отношения, но и обеспечить его безопасность, предотвратив негативное влияние как на самого ребенка, так и на игровое устройство. Вот несколько важных советов по безопасности в интернете, которые могут помочь родителям обеспечить комфортное времяпровождение детей во время игр:

1 Защищайте свои учетные записи в интернете с помощью надежных паролей и двухфакторной аутентификации.

Надежные пароли защищают учетные записи ваших детей от хакеров, которые могут попытаться получить доступ к конфиденциальной информации или связанным с ней способам оплаты (например, кредитной карте). Для большей эффективности включите двухфакторную аутентификацию (2FA). Это важная мера безопасности, которая требует ввода дополнительного кода при входе в учетную запись (обычно это одноразовый код, отправляемый на мобильное устройство).

Поговорите с ребенком о безопасности паролей. Дети должны знать основы безопасности в интернете, в частности, не сообщать никому свои пароли. Это касается и друзей, и авторитетных для ребенка лиц. Важно также отметить, что специалисты технической поддержки никогда не будут запрашивать логины и пароли к вашему личному кабинету в магазинах приложений или на онлайн-платформах.

2 Изучайте игры вместе и выбирайте проверенных разработчиков.

Родители не могут защитить своих детей в интернете, не владея информацией о том, в какие игры они играют. Один из лучших способов уберечь детей от вредоносного контента, кибербуллинга и вредоносных программ – обратить внимание на происхождение самих игр.

Все легальные игровые платформы предоставляют пользователям рейтинги и описания содержания игр, которые они размещают. Ресурсы, на которых размещаются пиратские или взломанные версии игр подобную информацию обычно не размещают. Это важно знать, потому что использование пиратских или «взломанных» версий игр – один из основных способов, с помощью которого хакеры могут склонить игроков к установке вредоносного ПО.

Как снизить риски при изучении игр:

- Внимательно изучайте пользовательское соглашение и политику обработки персональных данных игровых платформ и разработчиков игр, в особенности, в части обработки персональных данных (в том числе передачи их третьим лицам) и ограничения ответственности. В случае, если вы будете убеждены в сохранности личных данных (ваших и вашего ребенка), можно начинать установку игры.
- Вместе смотрите видеоролики игрового процесса. В интернете можно найти обзоры и видеозаписи игрового процесса практически любой игры в мире. Посмотрите популярные каналы в интернете, чтобы узнать, как выглядят игры.
- Никогда не используйте торрент-сайты для загрузки игр. Ни один легальный крупный издатель игр не использует торренты для распространения игр. Не запускайте файлы игр, загруженные с пиринговых торрент-сайтов.

3 Своевременно обновляйте программное обеспечение и устанавливайте настройки безопасности и родительского контроля игровой консоли.

Игровые консоли содержат настройки безопасности и родительского контроля, позволяющие ограничить доступ детей к играм, но не все они включаются автоматически. Например, по умолчанию Nintendo Switch поставляется со строгими настройками безопасности, в то время как консоли Sony Playstation и Microsoft Xbox более мягкие при заводских настройках.

4 Ограничьте возможность детей распространять личную информацию (например, через игровые метки или логины).

Дети, которые сообщают личные данные другим игрокам – даже просто используя свои настоящие имена или идентификационные данные в игровых метках – могут подвергать себя риску взлома, кражи персональных данных или преследований.

> Убедитесь, что ваши дети играют анонимно и не передают конфиденциальную, в том числе излишнюю личную информацию, другим игрокам: о времяпровождении, месте проживания, интересах, планах на отдых и т.д. В случае, если такая информация окажется в руках у киберпреступников, ребенок может подвергнуться не только хищению денежных средств, но и преследованию как в виртуальном, так и реальном мире.

5 Защитите свои устройства с помощью антивирусного ПО.

Загрузка видеоигр с авторитетных платформ снижает риски заражения вредоносным ПО, но не устраняет их. Например, компания Google постоянно удаляет игры[8], содержащие вредоносное ПО, из магазина Google Play, однако до момента удаления эти игры успевают попасть к сотням тысяч пользователей. В свою очередь игровая платформа Steam предоставляет[9] массу разнообразных защитных инструментов (включая аппаратные средства) для борьбы с кражей аккаунтов и распространением вредоносного ПО.

Надежное антивирусное решение способно защитить все ваши устройства от вредоносных программ и других вирусов – будь то поддельная онлайн-игра, фишинговая атака или что-то другое.

6 Грамотно выбирайте способы оплаты в приложениях.

Любая игра с внутриигровыми покупками (например, лутбоксы) сопряжена с дополнительными рисками. Если вы хотите ограничить расходы своих детей или предотвратить финансовые махинации в случае взлома их учетных записей, разумно используйте более безопасные способы оплаты, например, подумайте об открытии банковского счета специально для этих целей.

7 Установите временные ограничения для онлайн и мобильных игр.

Без ограничений по времени онлайн-игры могут стать отвлекающим фактором для ребенка, особенно для детей, которые уже страдают расстройствами внимания. Зацикленность на играх может быстро перерасти в зависимое поведение, когда дети игнорируют важные моменты своей жизни, чтобы продолжать играть.

В случае продажи или утилизации консоли/устройства удалите учетную запись и личные данные, сбросьте устройство до заводских настроек и уничтожьте накопитель (носитель) информации.

Передача устройства, с которого не были удалены персональные данные, покупателю в той же степени несет риск незаконного использования вашей личной информации и информации о ребенке посторонними лицами. Сброс настроек и очистка кэша смогут обеспечить невозможность восстановления, в том числе данных о ваших платежных инструментах, а также личной информации, которую ребенок мог указать в профиле или в отдельных играх.

Заключение

Несомненно, видеоигры для многих – это веселый способ провести время. Но если игровые персонажи и сюжетные линии по большей части – выдумка, то риски, связанные с онлайн-играми – реальны. Помимо множества честных геймеров есть и киберхулиганы, и хакеры, и похитители персональных данных, и преследователи.

Без надлежащих мер предосторожности и активного воспитания игровые привычки могут иметь серьезные негативные последствия, в том числе для вашей жизни и жизни ваших детей вне сети. Выполнение простых требований для обеспечения цифровой безопасности – верный способ минимизировать риски, связанные с играми в интернете.

автор
Полина Сурьянинова

[8] По данным компании Zednet: https://www.zdnet.com/article/google-play-malware-if-youve-downloaded-these-malicious-apps-delete-them-immediately/. Zednet – новостной аналитик в области технического оборудования и гейминга.

[9] По данным анализа Лаборатории Касперского: https://www.kaspersky.ru/blog/stealing-from-steam/3650/ (дата обращения: 27.09.2023).

Повышение культуры приватности в организации

Секреты эффективного обучения работников

Стремительное развитие цифровых технологий привело к тому, что они вошли практически в каждую сферу нашей жизни. Ежедневно, пользуясь различными социальными сетями, мессенджерами, интернет-платформами, мы передаем огромное количество персональных данных. Компании используют полученные данные для предоставления нам продуктов, сервисов, услуг, анализа наших потребностей, привычек, интересов, образа жизни. При этом для многих компаний персональные данные становятся ценнейшим информационным активом и источником дохода.

Наряду с активным развитием технологий наблюдается рост новых угроз информационной безопасности: причем нередко те инновационные решения, которые призваны защищать пользователей, сами несут для них риски утраты нарушения конфиденциальности, утечек личных данных. Именно об этом свидетельствует статистика.

По данным Роскомнадзора, в России с начала 2023 года[1]:

> **200** млн
записей о субъектах персональных данных скомпрометировано

177
уведомлений от компаний об утечках персональных данных получено

~70
случаев утечек подтверждено

При этом по состоянию на 2022 год, как отмечают в ведомстве[2]:

> **600** млн
записей оказалось в сети

~150
крупных утечек зафиксировано

87 %
случаев неправомерного распространения личной информации подтверждено

Целый ряд утечек 2022 года можно отнести к резонансным.

По данным Лаборатории Касперского, за первые пять месяцев 2023 года было обнаружено[3]:

197 млн
строк пользовательских данных

81 млн
строк с номерами телефонов

23 млн
строк с паролями

В 2022 году в результате[4]
168
значимых утечек

было опубликовано
> **2** млрд
записей

Согласно исследованию ГК InfoWatch, проведенному в финансовой сфере:

количество утечек выросло в **1,7** раза

> **80** %
утечек включают персональные данные

70 %
случаев – вина работников компании[5],

о чем также говорят представители Минцифры России[6].

[1] Сообщил заместитель главы Роскомнадзора Милош Вагнер информационному агентству ТАСС на Международном Петербургском экономическом форуме (данные по состоянию на 17 июня 2023 г.).

[2] Роскомнадзор зафиксировал около 150 крупных утечек персональных данных в 2022 году. Российская газета. URL: https://rg.ru/2023/01/30/kontrol-protechek.html (дата обращения: 27.09.2023).

[3] Утечки данных в России: в 2023 году злоумышленники не сбавляют обороты и меняют фокус внимания. URL: https://www.kaspersky.ru/about/press-releases/2023_utechki-dannyh-v-rossii-v-2023-godu-zloumyshlenniki-ne-sbavlyayut-oboroty-i-menyayut-fokus-vnimaniya (дата обращения: 27.09.2023).

[4] Значимые утечки данных в 2022 году. URL: https://go.kaspersky.com/ru-data-leakage-report-2022 (дата обращения: 27.09.2023).

[5] Финансовая сфера: утечки информации за 2022 год. InfoWatch. URL: https://www.infowatch.ru/analytics/analitika/finansovaya-sfera-utechki-informatsii-za-2022-god (дата обращения: 27.09.23).

[6] Причиной более 70% утечек информации становились сотрудники компаний. URL: https://iz.ru/1349104/2022-06-14/prichinoi-bolee-70-utechek-informatcii-stanovilis-sotrudniki-kompani (дата обращения: 27.09.2023).

При этом утечки затронули практически каждую сферу: государственные учреждения, промышленные предприятия, медицинские учреждение, научные организации, средства массовой информации, ритейл. В числе компаний, учреждений, организаций, у которых произошли утечки, имеются и те, которые получали данные не от самих субъектов, а от контрагентов/партнеров.

Среди причин утечек: небрежное отношение операторов к правилам обработки персональных данных и обеспечению их защиты, что усиливается отсутствием ответственности, соразмерной причиненному вреду. Для снижения количества утечек персональной информации любая компания, учреждение, организация, которые обрабатывают персональные данные, должны внедрить комплекс необходимых правовых, организационных и технических мер защиты.

Важной мерой является обучение работников компании тем правилам обращения с персональными данными, которые необходимы для обеспечения их безопасности. В частности, в данной статье мы расскажем:

- какой должна быть реализация требования по доведению до работников положений законодательства и локальных актов в части обработки и защиты персональных данных, чтобы это повлияло на снижение количества утечек из-за неправомерных действий/бездействия работников;
- достаточно ли доведения до работников текста закона и локальных актов или требуется более глобальный подход в виде комплексного обучения;
- как организовать эффективное обучение работников правилам ответственного отношения к персональной информации клиентов, сотрудников, иных субъектов, к которой они получают доступ в процессе ежедневной трудовой деятельности;
- каким образом выстроить обучение, чтобы оно было интересным;
- как привить работникам ответственный подход при работе с персональными данными и о многом другом.

С чего начать

> Первое, с чем стоит определиться: ограничиваться выдачей стопки документов сотруднику при приеме на работу и в случае изменения локальных актов – точно не лучшее решение.

Если компания ограничивается исключительно ознакомлением работников с требованиями законодательства и локальных актов, то в ежедневной рутине уровень важности данного вопроса для работников будет постоянно снижаться. Недостаточный уровень компетенций работников, незнание требований и мер по защите обрабатываемых данных, непонимание важности и смысла сохранности данных, а также безответственное отношение к обработке персональных данных может привести не только к утечке данных и вреду субъекту персональных данных, но и к краху репутации компании.

Для того, чтобы избежать подобных последствий, необходимо регулярно повышать уровень осведомленности работников по вопросам обработки и защиты персональных данных и развивать культуру приватности в компании.

Что на практике

На практике эффективность развития осознанного отношения к конфиденциальной информации, в том числе к персональным данным, к которым работники имеют доступ при выполнении трудовых обязанностей, зависит от количества и качества применяемых работодателем методов информирования и обучения работников, а также от адаптации методов под:

- «тип» работника (то есть нужно разделить информирование и обучение новых работников и тех, которые определенное время работают в компании);
- должность/выполняемые обязанности.

Адаптация методов под «тип» работника и должность/выполняемые обязанности

1. Новый работник. При приеме нового работника, помимо обязательного ознакомления под подпись с положениями законодательства и локальных документов, рекомендуется:

- подготовить и довести обучающие материалы с основными правилами ответственного отношения к конфиденциальной информации, включая персональные данные: например, можно сделать лекцию в курсе адаптации новых работников или отдельные видеоматериалы, статьи, в которых, помимо норм законодательства и локальных актов, будут практические примеры работы с конфиденциальной информацией и персональными данными – как можно и как нельзя;
- учесть при разработке обучающих материалов должность, на которую принимается работник, и обязанности, которые ему предстоит выполнять;
- рассказать о подразделении/конкретных экспертах, к которым можно обращаться за помощью по вопросам обеспечения кибербезопасности, включая вопросы обработки и защиты персональных данных;
- назначить на период адаптации/испытательного срока бадди/куратора, который также расскажет о важных правилах и их реализации с практической стороны.

> После окончания адаптационного периода/испытательного срока важно уделить время новому работнику и проверить эффект от проведенного обучения. Для подобных целей может быть полезна как личная встреча с работником, так и онлайн-тренинг длиной не более 30 минут с последующим тестом[7].

2. Действующий работник. Для действующих работников, помимо ознакомления с изменениями локальных актов по вопросам кибербезопасности, включая обработку и защиту персональных данных, необходимо предусмотреть инструменты регулярного повышения осведомленности в вопросах обработки и защиты персональных данных. Среди таких инструментов могут быть:

2.1. Обучающие программы

Одним из классических инструментов в современной реальности является онлайн-тренинг, в котором будет собрана вся необходимая информация по вопросам обработки и защиты персональных данных в компании. При составлении подобных программ стоит учитывать специфику деятельности работников. В частности, рекомендуется разделить их на четыре основные группы:

- работники, непосредственно осуществляющие обработку персональных данных/имеющие доступ к конфиденциальной информации[8];
- руководители;
- работники, задействованные в разработке/проектировании процессов;
- работники, выполняющие функции по обеспечению информационной безопасности/организации обработки и защите персональных данных.

В зависимости от того, какую из указанных «ролей» выполняет работник, следует выстраивать структуру и наполнение онлайн-тренинга или иной обучающей программы. В частности:

- для группы работников, которые непосредственно обрабатывают персональные данные/имеют доступ к конфиденциальной информации, рекомендуется разработать материалы, содержащие базовую информацию по вопросам обработки и защиты персональных данных, которая потребуется им при ежедневной работе;
- для руководителей целесообразно предусмотреть дополнительное специализированное обучение, поскольку их функционал предполагает контроль за соблюдением подчиненными работниками требований локальных актов по вопросам кибербезопасности, включая обработку и защиту персональных данных, а также ответственность за виновные действия/бездействие подчиненных работников;
- для группы работников, задействованных в проектировании и разработке новых продуктов и процессов, процесс обучения следует выстраивать с акцентом на реализацию принципов privacy by design[9] (иначе – думай о защите до начала реализации идеи);
- для группы работников, которые занимаются обеспечением кибербезопасности и специализируются на вопросах обработки и защиты персональных данных, рекомендуется предусмотреть возможность прохождения внешних обучающих программ/курсов (тестирования, экзамены, сертификации), а также участия в различных семинарах, конференциях, дискуссиях профессиональных сообществ.

[7] Рекомендуемое ограничение времени.

[8] Работники, которые обрабатывают персональные данные, но при этом не осуществляют функции организации обработки и защиты.

[9] Подход, при котором требование к обеспечению конфиденциальности данных учитывается на протяжении всего процесса-проектирования (то есть во всех бизнес-процессах на каждом этапе разработки). См.: Privacy by Design. The 7 Foundational Principles. Ann Cavoukian, Ph.D. URL: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf (дата обращения: 27.09.23).

> При этом стоит учесть: если инструментом повышения уровня приватности является внутренняя обучающая программа, по ее окончании рекомендуется провести тестирование, чтобы проверить уровень усвоения материалов.

2.2. Информационные рассылки и скринсейверы

Поддерживать высокий уровень осведомленности помогут также информационные рассылки и скринсейверы (заставки, которые отображаются на экране компьютера во время бездействия пользователя). Они могут быть, опять же, направлены на различные фокус-группы (иначе – адаптированы под должность/специфику деятельности работника).

Например, рассылки и скринсейверы с обзором последних изменений в области кибербезопасности, а также обработки и защиты персональных данных были бы полезны:

- работникам, осуществляющим функции обеспечения информационной безопасности и организации обработки и защиты персональных данных;
- руководителям.

В свою очередь, рассылки и скринсейверы о способах определения фишингового письма и порядке реагирования на него были бы полезны всем работникам.

2.3. Киберучения

Еще одним способом, который позволяет достичь ощутимых результатов в обучении при условии регулярного проведения, являются киберучения. Киберучения представляют собой процесс обучения работников противостоять атакам злоумышленников на примере реальных кейсов. То есть в рамках киберучений для работника искусственно создают ситуацию, в которой ему необходимо отразить «атаку злоумышленника».

Например, один из вариантов реализации киберучений – фишинговые рассылки, в рамках которых работникам направляются письма, содержащие учебную «вредоносную» ссылку или файл. Механизм прохождения киберучений при этом следующий: если работник не распознал фишинг и перешел по ссылке/открыл «вредоносный» файл, значит, не прошел обучение. Это будет сигналом для руководителя о необходимости повышения уровня знаний сотрудника в области кибербезопасности, включая обработку и защиту персональных данных. Если же не перешел по ссылке и удалил письмо – киберучение считается успешно пройденным.

2.4. Политика чистого стола

Еще один полезный метод – clean-desk policy («политика чистого стола»). Политика чистого стола – это одно из требований ISO 27001, ведущего международного стандарта по информационной безопасности. Ее суть можно объединить в одном важном правиле: уходя с работы, нужно оставить чистый стол.

Внедрение подобной политики – одна из лучших стратегий, которая помогает снизить риски неправомерного попадания конфиденциальной информации, в том числе персональных данных, к третьим лицам.

Для того, чтобы работники никогда не забывали принципы политики, можно подготовить наглядные информационные материалы-памятки и разместить их на рабочих местах, а также проверять, соблюдаются ли работниками эти принципы – не лежат ли в открытом доступе документы с персональными данными или ключи от помещений/шкафов, в которых такие документы размещены, не хранит ли работник на рабочем месте пароли и т.д. Для большей эффективности целесообразно предусмотреть порядок применения мер дисциплинарного взыскания за несоблюдение требований.

2.5. Игровой формат обучения

Закрепить эффект поможет игровой формат обучения. Например, можно провести игру по вопросам приватности между подразделениями/отделами компании. Для того, чтобы у сотрудников появилось желание участвовать, стоит придумать и анонсировать приз за высокие результаты. Призы могут быть:

- нематериальными (например, для победителей можно предусмотреть звания «Амбассадор privacy» или «Лидер privacy-культуры в организации»);
- материальными (мерч компании, сертификат на обед в ресторане и все, на что хватит фантазии[10]).

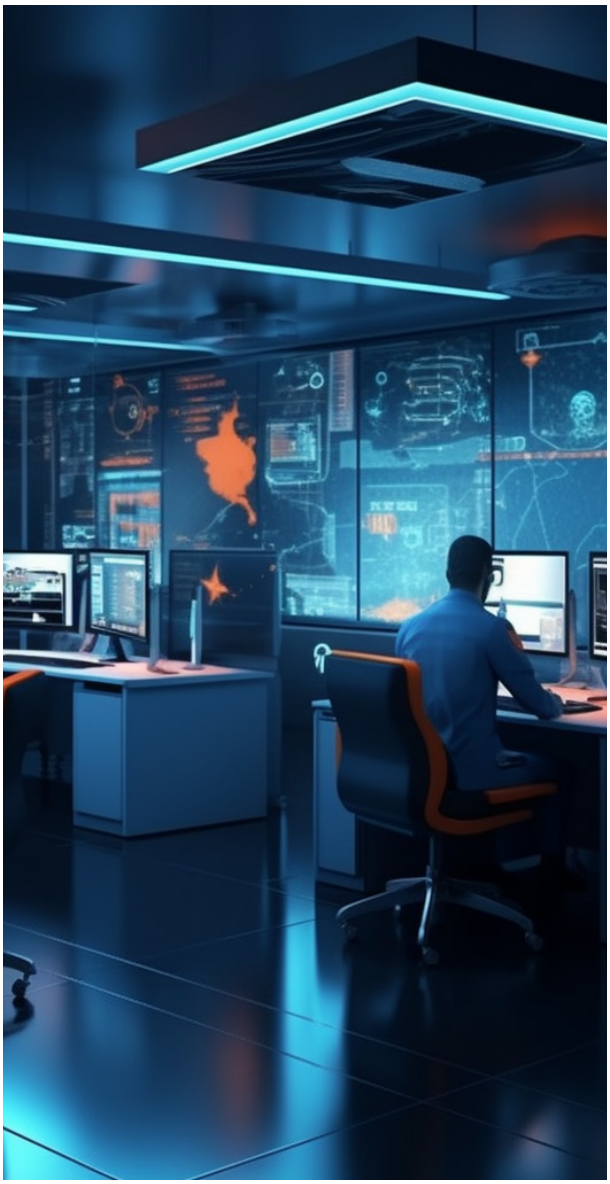
Подобный игровой формат не должен отнимать много времени от рабочего дня, чтобы каждый смог принять участие. Это могут быть privacy-квесты, марафоны, квизы, аналог игры «Что? Где? Когда?» и другие форматы. Перед началом каждого раунда игры стоит предоставлять работникам информационные материалы, с помощью которых они будут готовиться к новому туру.

Подведем итоги

Privacy-ориентированный подход к обучению работников и повышению уровня осведомленности в вопросах информационной безопасности, включая обработку и защиту персональных данных, может быть эффективным решением для повышения ответственности работников к тем данным, к которым они имеют доступ, в случае реализации комплексных мер. Среди таких мер:

- при приеме нового работника проводить плавное погружение в тему приватности и предоставлять практические инструменты, которые помогут соблюдать требования законодательства и локальных актов в части обеспечения информационной безопасности, а также обработки и защиты персональных данных;
- после прохождения испытательного срока проверять уровень полученных знаний с помощью онлайн-тренинга и/или теста;
- реализовывать обучающие мероприятия с проверкой полученных знаний для разных групп действующих работников;
- регулярно проводить киберучения;
- размещать на рабочих местах памятки по защите данных, реализовывать информационные рассылки, скринсейверы;
- применять «политику чистого стола»;
- внедрять игровой формат обучения (privacy-квесты, марафоны, квизы).

При этом рекомендуется не останавливаться на достигнутом и постоянно проверять эффективность проводимого обучения.



автор
Наталья Саенко

[10] Важно предусмотреть это в бюджете и урегулировать юридические тонкости проведения подобных мероприятий.

Обработка персональных данных, полученных в ходе телефонного разговора

Законно ли это и при каких условиях?

Телефонный разговор с потенциальными или действующими клиентами – способ коммуникации, который зачастую используют операторы. Цель такого взаимодействия может быть различной: принятие заявок на заключение договора, консультирование по действующим продуктам, сервисам, услугам, контроль качества обслуживания и не только. При этом, конечно же, в ходе телефонного разговора операторы могут запрашивать и получать персональные данные субъектов. Ключевой вопрос: законно ли это и что нужно делать оператору для того, чтобы обработка персональной информации, полученной таким путем, не нарушала права субъекта и позволяла оператору подтвердить правомерность своих действий.

Правомерность получения согласия по телефону

Согласие на обработку персональных данных, как следует из ч. 1 ст. 6 152-ФЗ[1], является одним из оснований (условий), которое позволяет оператору обрабатывать персональные данные. Вопрос в том, можно ли такое согласие получить по телефону. С формально-юридической точки зрения использование согласия в качестве основания обработки персональных данных по телефону допустимо. Это следует из ч. 1 ст. 9 152-ФЗ, согласно которой допускается любая форма получения согласия на обработку персональных данных, которая позволяет подтвердить факт его получения, если только специальная форма предоставления согласия прямо не предусмотрена законом.

Соответственно, в первую очередь оператору нужно понять: не подпадает ли процесс, связанный с обработкой персональных данных под это исключение – если нет, то он может использовать любую иную форму, в том числе получать согласие по телефону.

При этом оператор должен помнить о том, что для согласия, даже если оно получено в процессе телефонного разговора, ч. 1 ст. 9 152-ФЗ установлено пять основных квалифицирующих признаков:

- конкретность;
- предметность;
- информированность;
- сознательность;
- однозначность.

Конкретность предполагает отсутствие формулировок, которые не позволяют однозначно установить цели обработки персональных данных, перечень обрабатываемых персональных данных, а также факт совершения активных действий субъектом персональных данных, явно свидетельствующих о предоставлении согласия.

Предметность подразумевает наличие условий, которые позволяют сделать вывод о соответствии содержания обрабатываемых персональных данных целям обработки.

Информированность предполагает предоставление субъекту персональных данных всей необходимой и достоверной информации, которую оператор обязан ему предоставить.

Сознательность означает, что согласие должно быть осмысленным и обдуманным, а также должно отражать намерения субъекта персональных данных на предоставление такого согласия.

Однозначность представляет собой четкую последовательность фактов, связанных с обработкой персональных данных, а также перечня обрабатываемых данных.

Следовательно, каждый из этих признаков должен быть учтен оператором.

[1] Здесь и далее – Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Справочная правовая система «КонсультантПлюс».

Допустимые формы согласий на обработку персональных данных, получаемых по телефону

Еще один важный вопрос заключается в разграничении двух форм согласий: согласие, полученное в устной форме, и согласие, предоставленное путем конклюдентных действий, – а также в том, как эти формы реализовывать и какая наиболее предпочтительна.

Выбор формы получения согласия (устной или конклюдентной) остается на усмотрение оператора. Именно он с учетом специфики своей деятельности определяет, какая форма наиболее предпочтительна. Поскольку в силу закона у оператора есть обязанность по предоставлению доказательств наличия оснований на обработку персональных данных (ч. 3 ст. 9 152-ФЗ), реализовывать согласие нужно в той форме, которая в последующем не помешает ему подтвердить факт получения согласия.

Устная форма. Данный подход часто используется операторами при организации функционирования колл-центров – вполне закономерное решение, учитывая, что в случае с колл-центрами зачастую единственным способом получения согласия может быть телефонный разговор. Реализуя согласие в устной форме, важно учесть:

- устная форма должна сопровождаться словесным подтверждением волеизъявления субъекта на обработку персональных данных (иначе – субъект должен озвучить согласие);
- доказательством получения согласия может быть аудиозапись разговора[2], на которой зафиксирован факт предоставления согласия (о чем далее будет подробнее).

Пример предоставления согласия по телефону в устной форме приведен ниже (см. скрипт 1).

Конклюдентная форма. В юридической доктрине под конклюдентными (от лат. concludere – заключать) понимаются действия[3], которые явно свидетельствуют о намерении лица вступить в сделку[4]. Применительно к сфере персональных данных это означает действия, которые позволяют подтвердить намерение субъекта предоставить согласие на обработку персональных данных/согласиться с обработкой персональных данных. Примерами получения согласия в этом случае могут служить:

- проставление «галочки» пользователем в соответствующей веб-форме[5];
- факт размещения субъектом на каком-либо ресурсе информации о себе (например, резюме)[6]: при этом представляется важным в правилах использования интернет-ресурса прописать данный механизм предоставления согласия, а именно указать, что факт размещения согласия является подтверждением выражения воли субъекта на обработку размещаемой им информации;
- совершение определенных действий в процессе телефонного разговора (далее подробнее).

Пример предоставления согласия по телефону в форме конклюдентных действий приведен ниже (см. скрипт 2).

[2] Аудиозапись допускается при условии предварительного информирования об этом субъекта.

[3] Бездействие субъекта не может быть квалифицировано в качестве согласия на обработку персональных данных.

[4] Учебник: В 2 т. Т. I: Общая часть. Вещное право. Наследственное право. Интеллектуальные права. Личные неимущественные права / Отв. ред. Е.А. Суханов. – 2-е изд. – Статут, 2011. – 365 с.

[5] При условии логирования данного действия.

[6] Савельев А.И. Научно-постатейный комментарий к Федеральному закону «О персональных данных». 2-е издание, М.: Статут, 2021. С.186; Апелляционное определение Московского городского суда от 12 февраля 2019 г. по делу № 33-5265/2019.

Содержательная часть согласия и примеры скриптов

Ч. 4 ст. 9 152-ФЗ содержит неисчерпывающий перечень того, что должно включать согласие на обработку персональных данных, обличенное в письменную форму. Для устной и конклюдентной формы требований к содержательной части не установлено, поэтому при разработке согласий в указанных формах оператору необходимо руководствоваться общими требованиями к согласию – конкретность, предметность, информированность, сознательность, однозначность (подробнее – выше). Примеры реализации данных требований для устной и конклюдентной формы согласия приведены в скриптах 1 и 2.

Скрипт 01

Предоставление согласия в устной форме. «Для продолжения разговора подтвердите, что Вы даете согласие на обработку персональных данных, предоставленных Вами в процессе разговора, оператору [наименование/ФИО] в целях [...][7].

Более детально с условиями обработки персональных данных, сроками обработки и иной информацией Вы можете ознакомиться в Политике персональных данных на нашем сайте по интернет-адресу [...]. В случае несогласия разговор будет автоматически прекращен. Для подтверждения скажите «да»[8]».

(Клиент говорит да/нет).

Скрипт 02

Предоставление согласия в конклюдентной форме. «Для продолжения разговора нажмите «1», если Вы даете согласие на обработку персональных данных, предоставленных Вами в процессе разговора, оператору [наименование/ФИО] в целях [...].

Более детально с условиями обработки персональных данных, сроками обработки и иной информацией Вы можете ознакомиться в Политике персональных данных на нашем сайте по интернет-адресу [...]. Невыполнение действия по нажатию кнопки «1» в течение минуты влечет автоматическое завершение звонка»[9].

Обработка персональных данных, полученных в процессе телефонного разговора, в рамках заключения или исполнения договора

Помимо получения согласия по телефону, иным важным самостоятельным правовым основанием выступает договор, по которому субъект выступает стороной, выгодоприобретателем или поручителем, а именно заключение договора по инициативе субъекта или исполнение договора (п. 5 ч. 1 ст. 6 152-ФЗ).

В этой связи правомерность обработки персональных данных, полученных в результате телефонного разговора, может быть обусловлена, помимо согласия, также:

- исполнением обязательств по заключенному договору (например, это возможно, если субъект заключил с оператором договор и в дальнейшем хочет получить консультацию по вопросам его исполнения – при этом важно, чтобы обработка персональных данных не выходила за рамки цели, вытекающей из договора);
- инициативой на заключение договора (применимо в случае, если субъект только планирует заключить договор и перед его заключением предоставляет персональные данные).

Используя договор в качестве основания обработки персональных данных и формируя скрипты телефонных разговоров, стоит учесть положения п. 4 ст. 16 Закона о защите прав потребителей от 07.02.1992 № 2300-1 (далее – Закон о ЗПП):

[7] Цель определяет оператор персональных данных. Например, целью может быть предоставление определенного продукта, сервиса, конкретной услуги или подтверждение качества обслуживания.

[8] Может быть использовано иное слово, которое будет свидетельствовать о согласии клиента («согласен», «подтверждаю» и т.п.). Молчание или любое иное слово должны быть «сигналом» для представителя оператора к завершению разговора.

[9] Представителями Роскомнадзора также было отмечено, что допустимым способом получения согласия в конклюдентной форме является фраза: «Продолжая разговор, Вы даете согласие на обработку ваших персональных данных [имеются в виду данные, предоставляемые в процессе разговора – примечание автора]». См.: Вебинар Роскомнадзора «Защита персональных данных» от 27.07.2023 г. // VK Видео URL: https://vk.com/video-76229642_456239470 (дата обращения: 26.09.23).

«отказ потребителю в заключении, исполнении, изменении или расторжении договора с потребителем по причине его отказа предоставить свои персональные данные, за исключением случаев, если предоставление таких данных обусловлено законодательством, не допускается». Оператор также не может обосновывать необходимость получения персональных данных тем, что они являются встречным предоставлением по договору, поскольку предметы правового регулирования 152-ФЗ и Закона о ЗПП не пересекаются.

Бремя доказывания наличия оснований на обработку: что учесть

Как предусмотрено ч. 3 ст. 9 152-ФЗ, бремя доказывания факта наличия оснований на обработку персональных данных, в том числе их соответствия требованиям закона и получения от определенного субъекта, возлагается на оператора. Способы фиксации доказательств при этом определяет сам оператор. Представляется, для того, чтобы у оператора была возможность подтвердить наличие оснований на обработку, в локальных нормативных актах ему следует предусмотреть, в частности:

- способы фиксации доказательств;
- способы и сроки их хранения;
- порядок выгрузки из системы согласий/заявок на заключение договора;
- ответственных за хранение доказательств лиц;
- порядок доступа к соответствующим доказательствам.

Реализуя механизм предоставления согласия на обработку персональных данных или оставления заявки на заключение договора[10], оператору необходимо определиться: как он будет подтверждать, что телефонный разговор состоялся с соответствующим субъектом. Для этого, в частности, важно:

- осуществить идентификацию или аутентификацию субъекта (в зависимости от того, является субъект клиентом или нет): это возможно, например, по номеру телефона, с которого осуществляется звонок;
- зафиксировать метаданные разговора: в том числе, с какого номера был совершен звонок, в какое время, какой продолжительности;
- произвести запись содержания разговора, о чем предварительно предупредить субъекта[11].

> Важно иметь в виду: если субъект не является клиентом и звонит для получения консультации по продукту, услуге или сервису оператора, например, с целью его последующего заключения[12], основанием обработки персональных данных в таком случае будет инициатива на заключения договора. В случае, если субъект в дальнейшем отказался от заключения договора, оператор, в соответствии с ч. 5 ст. 21 152-ФЗ, обязан уничтожить персональные данные такого субъекта по причине достижения цели обработки персональных данных[13], но не позднее 30 дней с момента достижения цели.

Требования к срокам, в течение которых может храниться подтверждение наличия оснований обработки персональных данных

Соблюдение требований к срокам хранения персональных данных, в том числе к срокам хранения доказательств наличия оснований обработки персональных данных, необходимо, во-первых, для соблюдения прав субъектов, а во-вторых, для минимизации рисков, связанных с привлечением оператора к ответственности за нарушение требований законодательства РФ о персональных данных.

В первую очередь сроки хранения согласия на обработку персональных данных, заявки на заключение договора или самого договора определяются исходя из цели обработки персональных данных и, применительно непосредственно к согласию и договору, с учетом их условий. В последующем – то есть с момента истечения срока обработки персональных данных, указанного в согласии, срока действия заявки на заключение договора или срока действия договора – обработка персональных данных, в том числе хранение доказательств правомерности обработки, может осуществляться с учетом общего срока исковой давности. Такой срок составляет три года согласно ст. 197 Гражданского кодекса Российской Федерации (далее – ГК РФ)[14]. Основанием обработки при этом будет выступать уже не согласие или договор (его заключение/исполнение), а реализация прав и законных интересов оператора и третьих лиц (например, государственных органов) (п. 7 ч. 1 ст. 6 152-ФЗ).

[10] В случае, если в процессе оформления заявки по телефону предполагается предоставление персональных данных.

[11] Савельев А.И. // Научно-практический постатейный комментарий к Федеральному закону «О персональных данных» (2-е издание, переработанное и дополненное). «Статут», 2021. С.185-187.

[12] Цель: заключить договор, – должна явно считываться из телефонного звонка. Для этого, например, можно предусмотреть специальный канал коммуникации: для желающих заключить договор. В случае, если такая цель не считывается/отсутствует, использование инициативы на заключение договора в качестве основания обработки персональных данных не допускается.

[13] Например, целью может выступать предоставление субъекту продуктов, сервисов или услуг.

[14] Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // Справочная правовая система «КонсультантПлюс».

Привлечение оператора персональных данных к ответственности за неправомерную обработку персональных данных.

1 По инициативе субъекта персональных данных

Нормы ст. 17 152-ФЗ наделяют субъектов персональных данных правом на обжалование действий или бездействия оператора. Если субъект заявляет, что обработка персональных данных осуществляется неправомерно (в отсутствие правовых оснований), он вправе обратиться с иском в суд для привлечения оператора к гражданско-правовой ответственности. Реализуя такое право, субъект может потребовать возмещения убытков (ст. 15 ГК РФ) или компенсации морального вреда (ст. 24 152-ФЗ). При этом моральный вред компенсируется вне зависимости от того, возместил ли оператор убытки (реальный ущерб/неполученные доходы).

В качестве альтернативы субъект может защитить свои нарушенные права в административном порядке в соответствии с Федеральным законом от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации». Так, субъект может обратиться с жалобой в Роскомнадзор (то есть в уполномоченный орган по защите прав субъектов персональных данных).

2 По инициативе субъекта персональных данных

Оператор также может быть привлечен к ответственности по ст. 13.11 Кодекса об административных правонарушениях Российской Федерации (далее – КоАП РФ)[15]. Это возможно, например, в случае, если Роскомнадзор выявит соответствующие нарушения в ходе осуществления контрольно-надзорных мероприятий. Срок давности привлечения к ответственности при этом будет составлять один год со дня совершения административного правонарушения (п. 1 ст. 4.5 КоАП РФ).

Подтверждение оператором правомерности обработки персональных данных в судебном порядке

В случае выбора субъектом персональных данных судебного способа защиты своих прав оператор должен быть готов отстаивать правомерность обработки персональных данных в судебном порядке.

В качестве доказательств наличия таких оснований оператор, с учетом ст. 55 ГПК РФ, должен быть готов предоставить:

- аудиозапись (используя аудиозапись в качестве доказательства в суде важно, во-первых, обеспечить четкое и понятное качество записи и, во-вторых, для того, чтобы аудиозапись была признана допустимым доказательством, указать, кем и в каких условиях осуществлялась запись (ст. 77 ГПК РФ));
- письменные доказательства (в контексте данной статьи – транскрибацию: то есть перевод речи из аудиозаписи телефонного разговора в текстовую форму[16], которая будет дополнительным доказательством при предоставлении аудиозаписи в суд).

Заключение

Резюмируя все вышеизложенное, можно сделать следующие выводы:

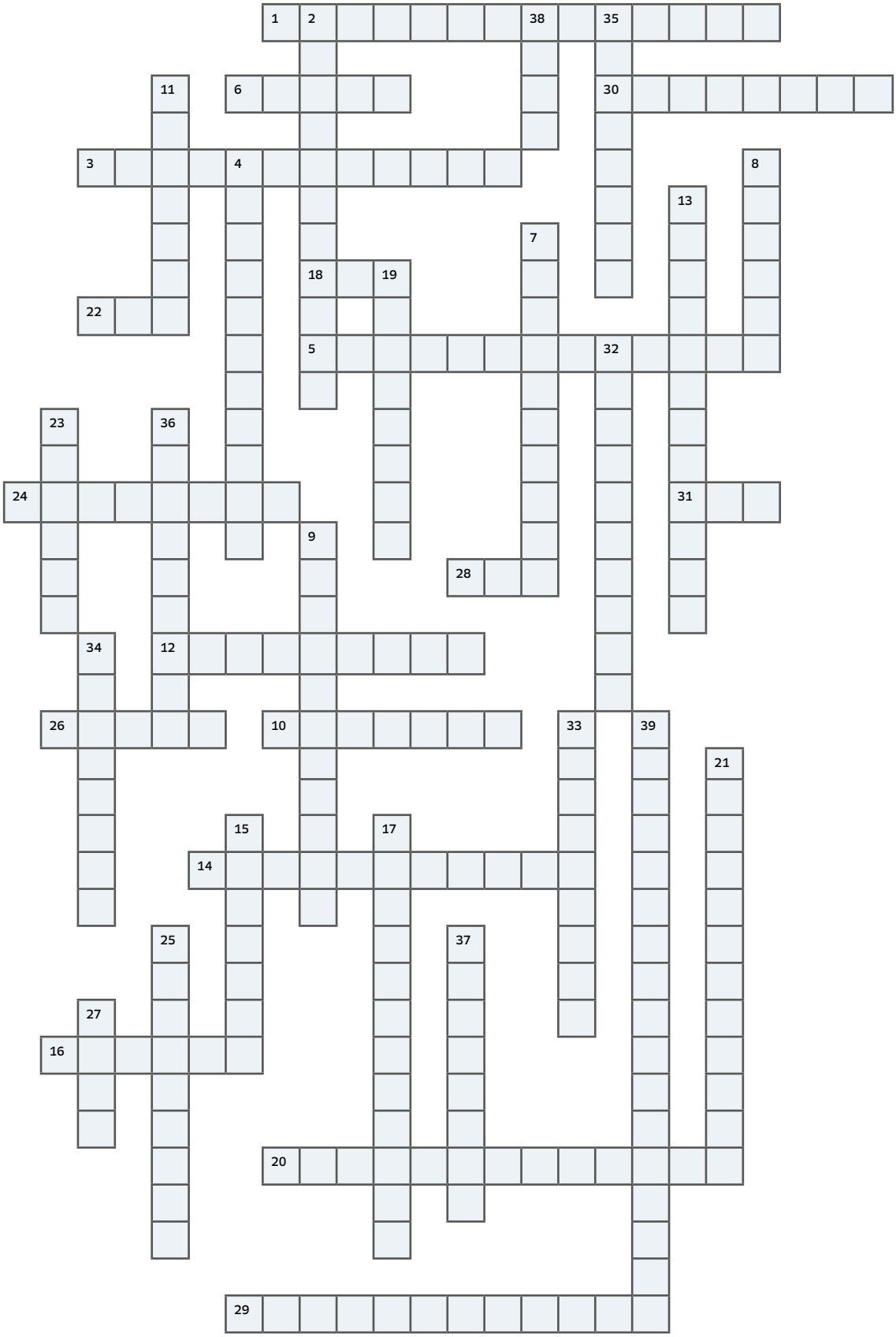
- обработка персональных данных на основании согласия или заявки на заключение договора, полученных в процессе телефонного разговора, допускается с учетом положений действующего российского законодательства;
- бремя доказывания получения согласия на обработку персональных данных/заявки на заключение договора по телефону возлагается на оператора;
- согласие на обработку персональных данных или заявка на заключение договора по телефону могут быть получены в устной форме или в форме конклюдентных действий в зависимости от действий, которые совершаются субъектом (озвучивание согласия, нажатие определенной кнопки);
- реализуя процесс получения согласий/заявок на заключение договора в устной или конклюдентной форме следует учесть рекомендации в части способов и сроков их хранения;
- для митигации правовых рисков оператору рекомендуется позаботиться о доказательствах подтверждения факта получения каждого из указанных оснований обработки персональных данных.

автор
Арина Гвоздырева

[15] Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // Справочная правовая система «КонсультантПлюс».

[16] Допускается не заверять транскрибацию, приложенную к аудиозаписи (См.: Определение СК по гражданским делам Верховного Суда Российской Федерации от 6 декабря 2016 г. № 35-КГ 16-18).

Privacy-кроссворд



По горизонтали:

1. Проверка принадлежности предъявляемого пользователем идентификатора и подтверждение его подлинности.

3. Дизайн пользовательского интерфейса, который намеренно могут использовать владельцы сайтов для побуждения пользователей совершать определенные действия, которые соответствуют интересам владельца сайта, но не отвечают потребностям пользователя (например, побуждение приобрести дополнительные ненужные услуги).

5. Уникальное обозначение сведений о лице, необходимое для определения такого лица и последующего установления его личности.

6. Принципы и стандарты поведения, которыми следует руководствоваться участникам отношений в сфере ИИ.

10. Технология, используемая Сбером в новогодней рекламе для создания образа Жоржа Милославского – персонажа фильма «Иван Васильевич меняет профессию».

12. Первая версия этой математической модели под названием «перцептрон» была представлена в конце 50-х годов XX века Фрэнком Розенблаттом.

14. Метод обеспечения безопасности данных, который преобразовывает их в зашифрованный вид.

16. Вид фишинга, при котором атака проводится с помощью телефонного звонка, в ходе которого злоумышленник использует психологические приёмы, побуждающие жертву раскрыть личные данные.

18. Цифровая платформа, которая позволяет идентифицировать человека по его биометрическим характеристикам – изображению лица и записи голоса.

20. Операция по обработке персональных данных, осуществляемая посредством следующих методов: применение идентификаторов, изменение состава данных, декомпозиция, перемешивание.

22. С адвокатом американской фирмы Levidow & Oberman Стивеном Шварцем эта программа сыграла злую шутку, когда он решил воспользоваться ею для подготовки материалов к судебному заседанию. Общее название программы: чат-…

24. Он лежал в основе немецкой шифровальной машины под названием Enigma, механизм работы которой разгадывал Алан Тьюринг – главный герой фильма «Игра в имитацию».

26. Информацию о нём, в частности, о его администраторе, можно узнать, например, посредством сервиса WHOIS.

28. Текстовые файлы, в которых хранится информация о действиях пользователей в информационной системе, а также информация о работе информационных систем.

29. Согласно 152-ФЗ, одной из составляющих обеспечения … является обнаружение фактов несанкционированного доступа к персональным данным и принятие соответствующих мер.

30. Обязанность лица, ответственного за организацию обработки персональных данных, связанная с проверкой соблюдения оператором и его работниками законодательства РФ о персональных данных и требований к защите.

31. Подтверждением факта уничтожения персональных данных является … об уничтожении персональных данных и выгрузка из журнала событий (если применимо).

33. Данные, относящиеся к этой категории, обладают определённым набором признаков: содержат характеристику физиологических или биологических особенностей человека, позволяют установить его личность и используется для этого оператором.

34. Набор правил, которые определяют способы передачи сообщений и обработки ошибок, с помощью которых различные программы обмениваются данными.

35. То, что было создано Лу Монтулли в 1994 г. при разработке браузера Netscape Navigator и используется сейчас для обеспечения работы сайтов и создания комфортных условий пользования.

36. То, что лежит в основе модели взаимодействия «оператор-обработчик».

37. Этим словом можно назвать злоумышленников, искусно проворачивающих преступные схемы с целью получения доступа к конфиденциальной информации, в том числе к персональным данным.

38. Система, предназначенная для оценки финансовых и не финансовых событий (банковских транзакций, операций с баллами лояльности и не только) на предмет их подозрительности и попадания под критерии мошеннических действий, называется системой анти-… мониторинга.

39. Совокупность методов и практик защиты систем и данных от атак злоумышленников, направленных на неправомерное получение доступа к конфиденциальной информации, включая персональные данные.

По вертикали:

2. Действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе.

4. В широком смысле это право на неприкосновенность частной жизни и личной информации.

7. Методы оценки и прогнозирования поведения человека на основе анализа, в том числе, его личных данных: интересов, предпочтений, привычек, – которые могут быть положены в основу «профиля» человека.

8. Персональные данные, полученные в результате математического преобразования биометрических персональных данных физического лица, содержащихся в единой биометрической системе.

9. Процесс предоставления пользователю или группе пользователей прав доступа, а также разрешений на выполнение определённых действий и привилегий в компьютерной системе.

11. В привычном понимании это теневой сегмент интернета.

13. Популярные архетипы героев в этой науке – Алиса, Боб и Ева, которая постоянно пытается подсмотреть их переписку.

15. Фишинговая атака, которая ориентирована на направление писем, содержащих вредоносные ссылки или зараженные вложения, в адрес высшего руководства компании, которые имеют доступ к наиболее конфиденциальной информации, с целью хищения денег, информации или реализации иных преступных намерений.

17. В свое время этот уполномоченный орган потребовал блокировки LinkedIn в России из-за нарушения требования российского законодательства, согласно которому при сборе персональных данных оператор обязан обеспечить запись, систематизацию, накопление, уточнение, извлечение персональных данных граждан России с использованием баз данных, находящихся в РФ.

19. Общее понятие для специальных категорий персональных данных, биометрических персональных данных и иных персональных данных.

21. Временное прекращение обработки персональных данных, которое производится при выявлении неправомерной обработки персональных данных или выявлении и подтверждении факта неточности персональных данных.

23. Модель предоставления повсеместного и удобного сетевого доступа «по требованию» к общему пулу конфигурируемых вычислительных сетей (сетей, систем хранения, приложений, сервисов).

25. Во второй и третьей части фильма «Матрица» главные герои Нео и Смит становятся зеркальными отражениями друг друга. Если Смит – это вирус Матрицы, то Нео – …

27. Юлий Цезарь изобрел собственную версию этой системы: каждую букву исходного текста он заменял на другую, отстоящую от нее по алфавиту на определенное число позиций. Адресату нужно было только знать точное число отступов.

32. Попытка выведения компьютерной системы из строя или получения доступа к информации, в том числе к персональным данным, за счет уязвимостей в устройстве или ПО.

Ответы

По горизонтали:

1. Аутентификация, **3.** Дарквиттеры, **5.** Идентификатор, **6.** Этика, **10.** Дипфейк, **12.** Нейросеть, **14.** Хэширование, **16.** Вишинг, **18.** ЕБС, **20.** Обезличивание, **22.** Бот, **24.** Алгоритм, **26.** Домен, **28.** Лог, **29.** Безопасность, **30.** Контроль, **31.** Акт

По вертикали:

2. Уничтожение, **4.** Приватность, **7.** Профайлинг, **8.** Вектор, **9.** Автоматизация, **11.** Дарквеб, **13.** Криптография, **15.** Уязвимость, **17.** Роскомнадзор, **19.** Сведения, **21.** Блокирование, **23.** Облако, **25.** Антивирус, **27.** Шифр, **32.** Кибератака, **33.** Биометрия, **34.** Протокол, **35.** Кукифайл, **36.** Получение, **37.** Мошенник, **38.** Фрод, **39.** Кибербезопасность

Рекомендации
от редколлегии

ЧТО ПОСМОТРЕТЬ?

Ретроспектива: антиутопия с приставкой «privacy».
Классический кинематограф о проблемах технологий и приватности.

Эта небольшая подборка из пяти фильмов открывает серию регулярных заметок о кинематографе, который поднимает вечные вопросы о том, что наш ждет в будущем, как развитие технологий размывает грани приватности, как это отразится на человеческом обществе и где граница между человеческим и искусственным разумом. Помимо общих тем, их объединяет еще одно – все они по праву заслужили статус «культовых». Их изучают в киношколах и на курсах по истории искусств, ими вдохновляются писатели и ИТ-стартаперы, их надо посмотреть хотя бы затем, чтобы понимать, откуда взялось «Черное зеркало» и «Мистер Робот».

Метрополис (Metropolis)

1927

Открывает список черно-белый немой фильм немецкого режиссера Фрица Ланга. Научно-фантастическая драма, полная метафор и экспрессии, о разделенном на две части обществе: высших элитарных слоях, проживающих в роскошных небоскребах, и рабочих, копошащихся в подземных фабриках, словно детали огромных машин, приказы которых они обязаны исполнять. Фредер Фредерсон, сын главного директора Метрополиса, случайно встречает Марию, лидера рабочего класса, после чего оказывается втянутым в борьбу за социальную справедливость и гармонию.

В «Метрополисе» впервые на большом экране был показан антиутопический город будущего, где технократическая элита занята эксплуатацией остального населения. Сочетая в себе потрясающую готическую эстетику и глубокий смысл, «Метрополис» остается одним из самых значимых фильмов начала 20-го века, который продолжает влиять на современное кино и искусство.

Цитата:

Посредником между головой и руками
должно быть сердце.

Источник

Бегущий по лезвию (Blade Runner)

1982

Фильм Ридли Скотта в жанре нео-нуар по роману пионера киберпанка Филипа Дика «Мечтают ли андроиды об электроовцах?» – одно из первых произведений кинематографа, в котором глубоко затрагиваются этические вопросы совместного существования живого и искусственного разума – людей и андроидов, а самое главное – как отличить первых от вторых, если внешне никакой разницы нет. Сюжет фильма разворачивается в мрачном и погруженном в постоянные дожди городе, где репликанты – андроиды, прислуживающие людям, становятся все более подобными человеку. Рик Декард (в прекрасном исполнении Харрисона Форда) назначен на последнее в его карьере задание по уничтожению группы беглых репликантов, которые представляют угрозу для общественной безопасности. В ходе своего путешествия Декард пытается разобраться с различными этическими дилеммами и вопросами о сущности человека и человечности.

Фильм, преисполненный цинизмом и пессимизмом (что, безусловно, роднит его с детективными голливудскими фильмами середины XX века), надолго стал эталоном для кинематографа в жанре киберпанк и антиутопия.

В 2017 году фильм обрел продолжение под названием «Бегущий по лезвию 2049» (режиссером стал Дени Вильнев), в котором те же философские вопросы поставлены под другим углом, с учетом того пути, что прошли технологии в реальном в мире с 1982 года.

Цитата:

Огонь, который горит в два раза ярче, сгорает в два раза быстрее.

Источник

Бразилия (Brazil)

1985

Источник

Фантастическая трагикомедия, созданная режиссером Терри Гиллиамом. Снятый в редком художественном стиле «дизельпанк» (все высокие технологии работают за счет двигателей внутреннего сгорания), фильм был вдохновлен романом Джорджа Оруэлла «1984» и произведениями Франца Кафки. Действие разворачивается в альтернативной реальности, где бюрократическое государство контролирует каждый аспект жизни обычных людей.

Главный герой, Сэм Лоури, работает в министерстве информации и страдает от монотонности и бюрократии своей работы. Все меняет одна опечатка в ордере на арест, который оформляется на невинного человека. Стремясь исправить последствия ошибки системы, главный герой оказывается втянутым в серию интриг, попутно сталкиваясь с искаженной этикой и моралью общества.

«Бразилия» – яркий пример критики бюрократических структур и потери индивидуальности в массовом обществе. Фильм воплощает мрачную и абсурдную атмосферу, создавая параллели с реальными проблемами современного общества.

Цитата:

Это справка о Вашем муже. А это справка, что я отдал Вам справку.

Джонни Мнемоник (Johnny Mnemonic)

1995

Один из «тяжеловесов» жанра киберпанк, научно-фантастический боевик, основанный на одноименном рассказе Уильяма Гибсона – человека, который этот жанр, собственно говоря, и создал.

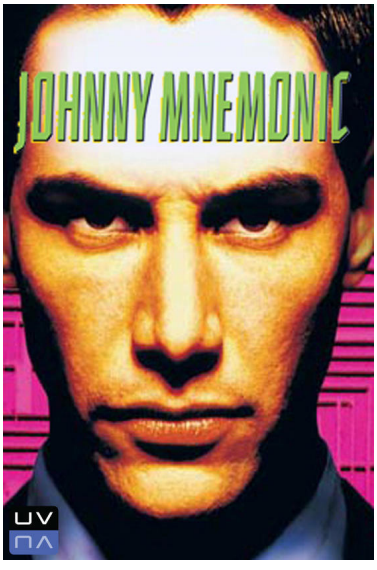
Фильм рассказывает о будущем, где информация стала самым ценным ресурсом, а люди имеют имплантированные в мозг специальные чипы для хранения данных. Главный герой, Джонни Мнемоник (второе слово – название профессии, а не фамилия), является курьером, который занимается перевозкой секретных данных в своем собственном мозгу. Он настолько преуспел в этом ремесле, что даже пожертвовал своими детскими воспоминаниями, чтобы «освободить место» для данных. Однако в ходе одного из особо сложных заданий он случайно загружает в мозг такое количество информации, которое превышает его емкость. Находясь на грани жизни и смерти, главный герой в ходе выполнения задания исследует темы технологического прогресса, личной идентичности и технологической этики.

Фильм получил смешанные отзывы от критиков, но тем не менее по праву стал культовым, представив зрителям мрачное будущее, где человеческая природа подвержена контролю, эксплуатации и зависимости от технологий, заставляя задуматься о последствиях технологического прогресса и нашей способности сохранить свою личность в мире, где все становится информацией.

Цитата:

– Ты в меня не выстрелишь.

– В голову – нет



Источник

Сеть (The Net)

1995

Источник

Первый кассовый фильм, в котором довольно убедительно (несмотря на сюжетные несостыковки и общую некоторую наивность происходящего) показано то, что позже назовут «цифровым профилем» и «кражей цифровой личности».

ИТ-аналитик Анджела Беннет (в исполнении Сандры Буллок) ведет затворнический образ жизни, но однажды переходит дорогу хакерской группировке и те в отместку полностью меняют ее личные данные во всех системах. И вот уже ее дом продан, рабочее место занято совершенно другим человеком и не узнают даже собственные (хоть и сетевые) друзья. И самое интересное – все окружающие думают, что все совершенно нормально, ведь все привыкли безоговорочно верить информации из государственных и корпоративных баз данных.

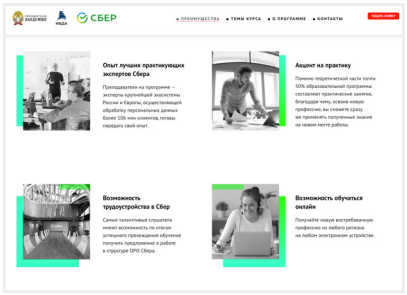
В отличие от других фильмов подборки, «Сеть» не рассуждает о сложных вопросах жизни и этики. По сути это «обычный» динамичный боевик из 90-х, которому суждено было стать пророческим.

Цитата:

Я – ничто, но они знали обо мне все. Они знали, что я ем, что я пью, где я родилась, какие фильмы я смотрела, какие сигареты я раньше курила... Они знали что до меня никому не будет дела, а когда кто-нибудь вспомнит – уже будет поздно.

ЧТО ИЗУЧИТЬ?

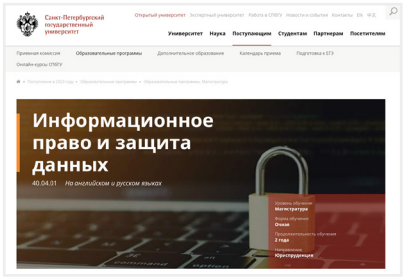
Обучающие программы, онлайн-курсы, вебинары



Программа профессиональной переподготовки «Эксперт в области обработки и защиты персональных данных»

Совместная практико-ориентированная онлайн-образовательная программа Института бизнеса и делового администрирования РАНХиГС и ПАО «Сбербанк». Программа направлена на подготовку экспертов в области организации обработки и защиты персональных данных. По итогам успешного завершения обучения выдается диплом профессиональной переподготовки установленного образца.

Ссылка



Магистерская программа Санкт-Петербургского государственного университета «Информационное право и защита данных»

С 1 сентября 2023 года на базе Санкт-Петербургского государственного университета реализуется магистерская программа «Информационное право и защита данных». Программа направлена на подготовку кадров в области информационных технологий и телекоммуникаций. Особое внимание уделяется изучению актуальных вопросов, касающихся «сквозных цифровых технологий», включая большие данные, искусственный интеллект, распределенные реестры. Одно из преимуществ программы – возможность выбора специального модуля по защите персональных данных, включающего дисциплины партнера СПбГУ ПАО «Сбербанк».

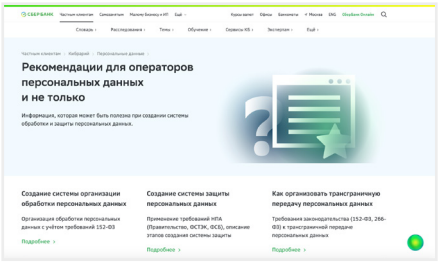
Научным руководителем программы является В. В. Архипов, имеющий многолетний опыт работы в практике по интеллектуальной собственности, информационным технологиям и телекоммуникациям международной юридической фирмы.

По окончании успешного завершения обучения выдается диплом государственного образца с присвоением квалификации «Магистр» по направлению подготовки 40.04.01.

Ссылка

ЧТО ПОЧИТАТЬ?

Рекомендации, статьи, книги



Рекомендации для операторов персональных данных и не только от экспертов Института DPO ПАО «Сбербанк»

Информация по вопросам создания системы организации обработки и защиты персональных данных, ориентированная на операторов персональных данных и представителей экспертного сообщества. Среди рекомендаций: вопросы построения системы организации обработки и защиты персональных данных, организация трансграничной передачи персональных данных, вопросы обработки и защиты персональной информации при использовании облачных сервисов, управление правовыми основаниями обработки персональных данных, порядок передачи информации об инцидентах с персональными данными.

Ссылка


ВЕСТНИК УДМУРТСКОГО УНИВЕРСИТЕТА 109
ЭКОНОМИКА И ПРАВО 2022. Т. 32, вып. 1

Правоведение

УДК 342.7

В.В. Архипов, В.Б. Наумов

ТЕОРЕТИКО-ПРАВОВЫЕ ВОПРОСЫ ОХРАНЫ ПРАВ ЧЕЛОВЕКА ПРИ ИСПОЛЬЗОВАНИИ БИОМЕТРИЧЕСКИХ ДАННЫХ СИСТЕМАМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ЕВРОПЕЙСКИЙ ОПЫТ[1]

В статье рассматриваются теоретические вопросы формирования правовых механизмов охраны прав человека, включая право на неприкосновенность частной жизни, в современных условиях цифровой трансформации. В работе на основе методов сравнительного правоведения исследованы правовые риски цифровизации в аспекте использования биометрических данных программными решениями и устройствами на базе технологии искусственного интеллекта. В результате проведенного исследования для повышения экономической эффективности технологий при одновременном обеспечении прав граждан с учетом растущего потенциала высоко персонализированного манипулирования и иных рисков технологии обработки биометрических персональных данных авторы приходят к выводам о значительных вызовах для права. Это усиливает значение выработки основных этических и правовых принципов в области искусственного интеллекта и формирования законодательной базы в сфере искусственного интеллекта.

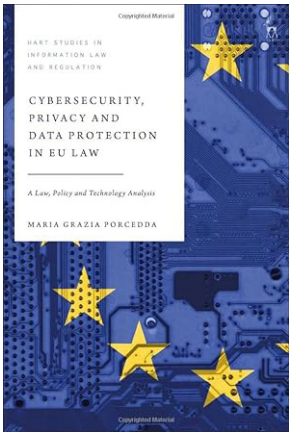
Ключевые слова: теория государства и права, теоретические основы цифровизации, права человека, неприкосновенность частной жизни, правовые риски, сравнительно-правовое исследование, цифровые технологии, цифровая трансформация, идентификация субъектов, биометрические данные, искусственный интеллект.

DOI: 10.35634/2412-9593-2022-32-1-109-118

Статья В. В. Архипова, В. Б. Наумова «Теоретико-правовые вопросы охраны прав человека при использовании биометрических данных системами искусственного интеллекта: европейский опыт»

«В статье рассматриваются вопросы формирования правовых механизмов охраны прав человека, включая право на неприкосновенность частной жизни, в современных условиях цифровой трансформации. На основе методов сравнительного правоведения исследованы правовые риски цифровизации в аспекте использования биометрических данных программными решениями и устройствами на базе технологии искусственного интеллекта.»[1].

Ссылка



Книга «Cyber Security, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis (Hart Studies in Information Law and Regulation)» by Maria Grazia Porcedda (Author)[2]

Книга описывает комплексный подход, сочетающий аспекты обозначения взаимосвязи между кибербезопасностью, неприкосновенностью частной жизни и защитой данных в законодательстве ЕС. В частности, рассматриваются противоречия, присущие политике кибербезопасности ЕС и ее реализации, поднимаются проблемы определения границ киберпространства и его безопасности. Также автором дается определение термину «данные» и поднимается вопрос определения ценности конфиденциальности и защиты данных.

Ссылка

[1] Из аннотации к статье.
[2] Перевод: «Кибербезопасность, конфиденциальность и защита данных в законодательстве ЕС: анализ закона, политики и технологий (исследования Харта в области информационного права и регулирования)». Автор: Мария Грация Порседда.

Privacy-Дайджест

Аналитика и обзор новостей в области персональных данных за третий квартал 2023 года

РОССИЙСКАЯ ФЕДЕРАЦИЯ

Вступили в силу:

Федеральные законы

1

Федеральный закон от 24 июня 2023 г. № 277-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» (вступил в силу 24.06.2023).

Цель изменений

Исключить использование информационных систем и/или программ для ЭВМ (в частности, иностранных мессенджеров) в определенных законодательством случаях.

Суть изменений

С 24 июня 2023 года КоАП РФ дополнен статьей 13.11.2, которая предусматривает административные санкции за использование принадлежащих иностранным юридическим лицам и/или иностранным гражданам информационных систем и/или программ для ЭВМ в случаях, когда в отношении такого использования установлен запрет.

Санкции будут применяться при наступлении следующих обстоятельств:

1. *лицом, использующим информационную систему и/или программу для ЭВМ, является:*
   - *государственная компания;*
   - *государственное или муниципальное унитарное предприятие;*
   - *публично-правовая компания или хозяйственное общество, в уставном капитале которых доля участия РФ, субъекта РФ или муниципального образования в совокупности превышает 50%;*
   - *кредитная организация;*
   - *некредитная финансовая организация (если она осуществляет деятельность, указанную в ч. 1 ст. 76.1. Федерального закона от 10.07.2002 № 86-ФЗ «О ЦБ РФ»);*
   - *субъект национальной платежной системы[1];*
2. *информационные системы и/или программы для ЭВМ принадлежат иностранным юридическим лицам и/или иностранным гражданам (соответствующий Перечень опубликован на официальном сайте Роскомнадзора);*
3. *указанные информационные системы и/или программы для ЭВМ используются для обмена электронными сообщениями между пользователями этих информационных систем и/или программ, при котором отправитель электронного сообщения самостоятельно определяет получателей, и при этом информация, обмен которой происходит, не размещается в сети «Интернет» в открытом доступе (то есть не является общедоступной);*

[1] В связи с тем, что запрет, согласно ч. 8 ст. 10 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технология и о защите информации», распространяется именно на указанных лиц (далее – 149-ФЗ). Норма введена в действие Федеральным законом от 29.12.2022 № 584-ФЗ, вступила в силу с 01.03.2023.

4. *обмен электронным сообщениями осуществляется в одном или нескольких перечисленных случаях – при предоставлении государственных и муниципальных услуг, выполнении государственного или муниципального задания, при реализации товаров, работ, услуг, имущественных прав;*
5. *указанный обмен производится для передачи платежных документов и/или предоставления информации, содержащей персональные данные граждан РФ, данные о переводах денежных средств в рамках применяемых форм безналичных расчетов, сведения, необходимые для осуществления платежей и/или сведения о счетах (вкладах) граждан РФ в банках.*

Размер административного штрафа в случае нарушения будет составлять:

- *от 30 000 до 50 000 рублей для должностных лиц;*
- *от 100 000 до 700 000 для юридических лиц.*

Значение изменений

Лицам, подпадающим под запрет ч. 8 ст. 10 149-ФЗ (указаны выше), необходимо оценить все процессы компании на предмет подпадания под обстоятельства, обозначенные в п. 2)-5). В случае, если каждое из обстоятельств присутствует в процессе, необходимо пересмотреть процесс, а именно исключить использование иностранных информационных систем и/или программ для ЭВМ.

Ссылка

2 Федеральный закон от 31 июля 2023 г. № 406-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Федеральный закон «О связи» (вступил в силу 31.07.2023, отдельные положения вступают в силу с 01.12.2023, 01.02.2024, 01.09.2024)[2].

Цель изменений

Определить ограниченный перечень способов, которые могут применяться владельцами сайтов/страниц сайтов, информационных систем и программ ЭВМ для авторизации пользователей, находящихся на территории РФ.

Суть изменений

С 01 декабря 2023 года в статью 8 149-ФЗ вводится новая часть 10, положениями которой будут закреплены способы авторизации пользователей на сайтах, в информационных системах, программах ЭВМ, принадлежащих российским владельцам[3]. Среди способов, которые смогут применять владельцы сайтов, информационных систем, программ для ЭВМ:

- *использование абонентского номера российского оператора связи[4];*
- *использование портала «Госуслуги»;*
- *использование ЕБС в порядке, предусмотренном 572-ФЗ[5];*
- *использование иной информационной системы, которой владеет российское юридическое лицо или российский гражданин.*

[2] Законом вносится ряд изменений, в дайджесте рассматриваются те, которые относятся к сфере персональных данных.

[3] Владелец сайта в сети «Интернет» – лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети «Интернет», в том числе порядок размещения информации на таком сайте (п. 17 ст. 2 149-ФЗ).

[4] Поскольку операторами подвижной радиотелефонной связи могут быть только российские лица (ч. 4 ст. 12 Закона № 99-ФЗ и п. 4 Положения о лицензировании деятельности в области оказания услуг связи (утв. Постановлением Правительства РФ от 30.12.2020 N 2385), п. 2 ст. 30 Закона № 126-ФЗ).

[5] Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // Справочная правовая система «КонсультантПлюс».

Важно: определение понятия «авторизация» на текущий момент в 149-ФЗ отсутствует. По общему правилу, под авторизацией допустимо понимать процесс предоставления пользователю доступа в компьютерной системе, в соответствии с правами доступа, определенными для этого пользователя в ней (что отличает указанное понятие от понятий аутентификации и идентификации). До уточнения значения термина «авторизация» применительно к вносимым изменениям под авторизацией рекомендуется понимать и процедуру регистрации, и процедуру входа на ресурс.

Значение изменений

Исключение возможности использовать для авторизации пользователей на сайтах, в информационных системах, программах ЭВМ, принадлежащих российским владельцам, способы, не определенные положениями 149-ФЗ.

Ссылка

3 Федеральный закон от 31 июля 2023 г. № 408-ФЗ «О внесении изменения в Федеральный закон «Об информации, информационных технологиях и о защите информации» (вступил в силу с 01.10.2023).

Цель изменений

Сделать механизмы рекомендательных технологий прозрачными, не допускать их использование в незаконных целях, а также обеспечить защиту прав и законных интересов пользователей в сети «Интернет» от злоупотреблений со стороны владельцев сайтов и/или страниц сайта в сети «Интернет», информационных систем, программ для ЭВМ (далее – информационные ресурсы).

Суть изменений

** Рекомендательные технологии – информационные технологии предоставления информации на основе сбора, систематизации и анализа сведений, относящихся к предпочтениям пользователей сети «Интернет», находящихся на территории РФ.*

В Федеральный закон «Об информации, информационных технологиях и о защите информации» включена статья 10.2.2. Среди ключевых изменений, которые вводятся данной статьей с 01 октября 2023 г.:

1. *Введена обязанность владельца информационного ресурса[6] информировать пользователей о применении на информационном ресурсе рекомендательных технологий и определены критерии, соблюдение которых позволяет применять рекомендательные технологии. Среди критериев:*
   - *разместить на информационном ресурсе правила применения рекомендательных технологий, соответствующие требованиям ст. 10.2.2. 149-ФЗ и регулятора[7], и обеспечить беспрепятственный[8] и безвозмездный доступ к ним;*
   - *описать процессы и методы сбора, систематизации, анализа сведений, относящихся к предпочтениям пользователей сети «Интернет», способов осуществления таких процессов и методов (подлежит включению в правила применения рекомендательных технологий);*

[6] Требования не распространяются на операторов ГИС, государственные органы и органы местного самоуправления.

[7] Требования должны быть установлены Роскомнадзором. Подробнее – Ссылка.

[8] Доступ не должен быть ограничен или обусловлен регистрацией или идентификацией пользователя.

- *описать виды (перечень) сведений, относящихся к предпочтениям пользователей сети «Интернет», которые используются для предоставления информации с применением рекомендательных технологий, а также источники получения таких сведений (также подлежит включению в правила применения рекомендательных технологий);*
- *обеспечить информирование пользователей сети «Интернет» о применении на информационном ресурсе рекомендательных технологий*[9].

2. *В случае выявления нарушений указанных требований Роскомнадзор вправе запросить у владельца информационного ресурса информацию о применении рекомендательных технологий, а также доступ к программно-техническим средствам рекомендательных технологий для проведения оценки соответствия их применения устанавливаемым Роскомнадзором требованиям.*
3. *Владелец ресурса обязан предоставить запрашиваемую информацию и доступ к программно-техническим средствам в течение 10 дней со дня получения уведомления Роскомнадзора или в иной установленный в уведомлении срок.*
4. *В случае непринятия владельцем ресурса в течение 24 часов с момента получения уведомления мер по устранению нарушений Роскомнадзор направляет оператору связи требование о принятии мер по ограничению доступа к информационному ресурсу, а оператор связи обязан незамедлительно ограничить доступ к ресурсу.*
5. *Если в последующем владелец ресурса принял меры по устранению нарушений, он направляет в Роскомнадзор соответствующее уведомление, а Роскомнадзор проверяет его достоверность и далее, при условии достоверности полученных сведений, направляет оператору связи уведомление о возобновлении доступа к ресурсу, которое оператор связи обязан выполнить.*
6. *Нарушение владельцем информационного ресурса требований 149-ФЗ в части применения рекомендательных технологий влечет за собой уголовную, административную и иную ответственность в соответствии с законодательством РФ.*

Значение изменений

Владельцам информационных ресурсов, использующим рекомендательные технологии, необходимо привести сайты, страницы сайтов, информационные системы, программы для ЭВМ, на которых задействованы такие технологии, в соответствие с новыми требованиями законодательства. В случае невыполнения требований, во-первых, появляется риск ограничения доступа к ресурсу, во-вторых, риск привлечения к ответственности.

Ссылка

[9] Роскомнадзор рекомендует разместить на информационном ресурсе сообщение следующего содержания: «На информационном ресурсе применяются рекомендательные технологии». Ссылка

Подзаконные акты

1

Указ Президента РФ от 18.09.2023 № 695 «О представлении сведений, содержащихся в документах, удостоверяющих личность гражданина Российской Федерации, с использованием информационных технологий» (вступил в силу с 18.09.2023).

Цель изменений

Совершенствование порядка предъявления документов, удостоверяющих личность гражданина РФ, и иных документов с использованием информационных систем.

Суть изменений

Гражданам РФ предоставляется возможность использовать «цифровой паспорт». Это значит, что представление гражданами РФ документов, удостоверяющих личность гражданина РФ, и иных документов, выданных гражданам РФ государственными органами РФ, в электронной форме через приложение «Госуслуги» будет приравниваться к предъявлению указанных документов. Использование «цифрового паспорта» при этом – добровольное решение.

Нововведение будет распространяться на случаи представления документов, определенных Правительством РФ. Правительству РФ в течение трех месяцев (срок с момента вступления Указа в силу) необходимо, в частности, определить:

- *перечень документов, которые могут предъявляться с использованием мобильного приложения «Госуслуги»;*
- *порядок использования мобильного приложения;*
- *состав сведений, которые могут быть представлены с использованием мобильного приложения;*
- *порядок обработки указанных сведений.*

На Минцифры России возлагается обязанность по ведению реестра юридических лиц, которые в своей деятельности используют сведения, предоставляемые через мобильное приложение.

Значение изменений

Юридическим лицам, в том числе операторам персональных данных, предстоит включиться в реестр, содержащий данные о юридических лицах и видах деятельности, для которых используются сведения, представленные с использованием мобильного приложения. До момента включения в реестр не допускается осуществлять проверку сведений о гражданине РФ посредством мобильного приложения «Госуслуги».

Ссылка

2

Постановление Правительства РФ от 19 августа 2023 г. № 1356 «О внесении изменения в Правила принятия решения уполномоченным органом по защите прав субъектов персональных данных о запрещении или об ограничении трансграничной передачи персональных данных в целях защиты нравственности, здоровья, прав и законных интересов граждан» (вступило в силу 19.08.2023).

Цель изменений

Уточнение порядка рассмотрения уведомлений о трансграничной передаче персональных данных.

Суть изменений

В случае, если оператор персональных данных взамен ранее направленному уведомлению о трансграничной передаче персональных данных направляет новое уведомление, ранее поступившее уведомление рассмотрению Роскомнадзором не подлежит, а новое уведомление

рассматривается в соответствии с порядком, определенным Постановлением Правительства РФ от 16.01.2023 № 24 «Об утверждении Правил принятия решения уполномоченным органом по защите прав субъектов персональных данных о запрещении или об ограничении трансграничной передачи персональных данных в целях защиты нравственности, здоровья, прав и законных интересов граждан».

Роскомнадзор об этом уведомляет оператора в течение трех дней с даты получения вновь поступившего уведомления любым доступным способом, который позволяет подтвердить факт получения оператором ответа (в том числе допускается направление ответа по адресу, указанному в уведомлении оператора).

Значение изменений

Если оператору персональных данных потребуется изменить информацию по ранее направленному уведомлению о трансграничной передаче, появляется возможность направить новое уведомление с более актуальными данными. Пояснение: вводимое правило действует в течение срока рассмотрения Роскомнадзором уведомлений и не применяется к случаям, когда ранее направленное уведомление было рассмотрено Роскомнадзором.

Ссылка

3 Распоряжение Правительства Российской Федерации 4 июля 2023 г. № 1790-р (вступило в силу с 04.07.2023).

Цель изменений

Уточнить порядок проведения эксперимента по авторизации пользователей на сторонних интернет-ресурсах через ЕСИА[10].

Суть изменений

Среди ключевых изменений – расширение:

- *перечня сведений, которые владельцы программ ЭВМ, сайтов, используемых для функционирования социальных сетей, агрегаторов, информационных ресурсов по поиску работы, могут собирать с согласия граждан (пользователей указанных ресурсов) с помощью ЕСИА.*
- *а также целей, в которых указанные сведения могут собираться[11].*

Изменения распространяются на участников эксперимента об авторизации пользователей через ЕСИА (то есть на всех, кто использует ЕСИА для авторизации пользователей и включен в перечень участников эксперимента). Цели и сведения определяются индивидуально для каждого участника эксперимента.

Значение изменений

У участников эксперимента появляется возможность с согласия граждан собирать большее количество сведений в большем количестве целей, что предполагает, в частности, расширения спектра возможностей, которые может предоставить онлайн-ресурс пользователю с использованием ЕСИА.

Ссылка

[10] Эксперимент начался 01.04.2021 и продлится до 31 декабря 2023 года.

[11] Примеры целей: создание аккаунта пользователя, восстановление доступа к аккаунту пользователя, заключение договоров аренды объектов недвижимости и др.

4

Приказ Росархива от 31 июля 2023 г. №77 «Об утверждении Правил организации хранения, комплектования, учета и использования документов Архивного фонда Российской Федерации и других архивных документов в государственных органах, органах местного самоуправления и организациях» (вступил в силу с 31.07.2023).

Цель изменений

Определить актуальные правила организации, хранения, учета и использования документов Архивного фонда РФ и других архивных документов.

Суть изменений

Определены актуальные правила организации, хранения, учета и использования документов Архивного фонда РФ и других архивных документов, в частности, требования к хранению электронных документов, требования к помещениям, в которых они хранятся. В самостоятельных разделах размещены правила проведения экспертизы ценности документов, оформления результатов экспертизы. Актуализированы формы документов, которые необходимо использовать при комплектовании архивов.

Ранее такие правила были утверждены Минкультуры России, однако соответствующие полномочия на текущий момент переданы Росархиву.

Значение изменений

С момента вступления в силу Приказа организация работы с архивными документами должна осуществляться в соответствии с новыми правилами.

Ссылка

5

Постановление Правительства РФ от 1 сентября 2023 г. № 1429 «О внесении изменений в Положение о единой биометрической системе, в том числе о ее региональных сегментах» и Постановление Правительства РФ от 01.09.2023 № 1430 «О внесении изменений в некоторые акты Правительства РФ» (вступают в силу с 01.01.2024 г.).

Цель изменений

Предоставить гражданам РФ возможность управлять согласиями на обработку биометрических персональных данных через ЕСИА.

Суть изменений

С 1 января 2024 года гражданам предоставляется возможность управлять своими согласиями на обработку биометрических персональных данных через единую систему идентификации и аутентификации (ЕСИА). В Личном кабинете у пользователя ЕСИА появятся все согласия на обработку его биометрических персональных данных, предоставленные аккредитованным государственным органам, органам местного самоуправления, Банку России, организациям финансового рынка, иным организациям, индивидуальным предпринимателям, нотариусам, операторам региональных сегментов единой биометрической системы с использованием личного кабинета на ЕСИА.

Значений изменений

Операторы должны предусмотреть возможность отзыва субъектом согласия на обработку его биометрических персональных данных без непосредственного взаимодействия с оператором в процессах, в рамках которых осуществляется обработка биометрических персональных данных.

Ссылка (1)

Ссылка (2)

ЕВРОПЕЙСКИЙ СОЮЗ

1

3 июля 2023 г. Агентство Европейского Союза по вопросам кибербезопасности (ENISA) опубликовало Стандарты по цифровой идентификации (Digital Identity Standards).

Суть изменений

В документе раскрыто понятие цифровой идентификации, а также проведен анализ наиболее важных мер стандартизации в области цифровой идентификации. Наибольшее внимание уделено средствам идентификации, создаваемым и управляемым европейскими службами доверия, и кошельку цифровой идентификации Европейского Союза[12].

Ссылка

2

17 июля 2023 г. Центр Европейской политики (European Policy Center) опубликовал документ под названием «План обеспечения квантовой кибербезопасности для Европы» («A quantum cybersecurity agenda for Europe»).

Суть изменений

В документе изложены ключевые рекомендации по обеспечению защиты ЕС от квантовых атак[13], среди которых:

- *разработка плана скоординированных действий ЕС по квантовому переходу;*
- *создание профильной экспертной группы в рамках Агентства по сетевой и информационной безопасности Европейского Союза (ENISA) с национальными экспертами для обмена опытом;*
- *определение приоритетов для перехода на постквантовое шифрование и обеспечение криптографической гибкости для реагирования на возникающие угрозы;*
- *обеспечение политической координации между Европейской комиссией, государствами-членами ЕС, агентствами национальной безопасности и ENISA для определения технологических приоритетов и вариантов использования квантово-безопасных технологий;*
- *содействие технической координации для устранения пробелов в профильных исследованиях;*
- *определение возможности использования «песочниц» для ускорения разработки приложений на основе квантовых информационных технологий.*

Ссылка

[12] С помощью данного инструмента осуществляется виртуальная идентификация, которая необходима для получения государственных и частных услуг (в том числе для открытия банковского счета), регистрации на сервисах, подтверждения возраста субъекта персональных данных.

[13] Попытка взлома, за которой стоит возможность квантовых компьютеров получить доступ к зашифрованной информации. Чаще всего имеется в виду случай, когда за счет сверхвычислительной мощности квантовый компьютер используется для того, чтобы расшифровать hash-функцию, применяемую для защиты (например, в блокчейне или ассиметричном шифровании при построении электронной подписи).

АЗИЯ

1 24 июля 2023 г. Народный банк Китая («НБК») опубликовал проект правил по управлению безопасностью данных «Меры по управлению безопасностью данных в сферах бизнеса, подпадающих под юрисдикцию НБК».

Суть изменений

Документ регулирует обработку электронных данных, собранных и сгенерированных в ходе предпринимательской деятельности, которые находятся под наблюдением и контролем НБК (регулируемые операции). Такие регулируемые операции по обработке данных в основном включают те, которые осуществляются в следующих областях бизнеса:

- *денежно-кредитная политика;*
- *трансграничные операций в юанях;*
- *межбанковские операции;*
- *статистика финансовой отрасли, платежей и клиринга;*
- *управление валютой и цифровыми юанями;*
- *управление казначейством;*
- *сбор кредитов и борьба с отмыванием денежных средств.*

Ссылка

2 11 августа 2023 г. в Индии принят всеобъемлющий закон о защите данных – Digital Personal Data Protection Act, («DPDP Act»).

Суть изменений

Закон DPDP применяется к персональным данным, позволяющим идентифицировать владельца данных, которые либо собираются в цифровом виде, либо переводятся в цифровой вид после их сбора в нецифровом виде. Закон DPDP не распространяется на персональные данные, обрабатываемые в личных или бытовых целях и на агрегированные персональные данные, собранные для исследовательских и статистических целей, которые не используются для принятия каких-либо решений, касающихся конкретного субъекта персональных данных.

Ссылка

3 18 июля 2023 г. Сингапурская комиссия по защите персональных данных («PDPC») опубликовала проект Руководящих принципов по использованию персональных данных в случае их применения для обучения систем искусственного интеллекта.

Суть изменений

Руководящие принципы направлены на разъяснение положений Сингапурского закона о защите персональных данных («PDPA») 2012 года в контексте разработки и внедрения систем искусственного интеллекта, предполагающих использование персональных данных для автономного принятия решений или для оказания содействия, в том числе путем предоставления прогнозов, в принятии решений лицам, которые такие решения принимают.

Ссылка

Редколлегия

SBER PRIVACY JOURNAL

Первое издание в России, посвященное персональным данным и приватности, которое выпускают специалисты Сбербанка

SBER BANK PRIVACY

Узнайте больше о том, как Банк обрабатывает и защищает персональные данные

КИБРАРИЙ. ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Что нужно для того, чтобы минимизировать риски, связанные с обработкой персональных данных?

SBER PRIVACY
JOURNAL

СБЕР КИБЕР БЕЗОПАСНОСТЬ

ВЫПУСК №6 | СЕНТЯБРЬ 2023