Гафарова Раиля Раилевна, Магистрант,
Поволжский государственный университет сервиса,
Тольятти

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Аннотация: Для любой организации – любого юридического лица – вопрос защиты персональных данных стоит на приоритетном месте. Данная статья посвящена особенностям и средствам защиты персональных данных в информационных системах, а также ходу действий ответственного субъекта, планирующего обработку персональных данных.

Ключевые слова: персональные данные, информационная система, актуальные угрозы, технические и организационные меры, криптографические средства, последовательность действий

Область защиты персональных данных регулируется законодательным правом (одной из подотраслей административного права), нормы которого прописаны в законодательных актах. Один из основных – Федеральный закон № 152-ФЗ от 27.07.2006 «О персональных данных» [1].

Реализация мер по защите персональных данных – ответственность субъекта, который собирает и обрабатывает данные в информационной системе. Как правило, таким субъектом выступает компания, которая владеет базами данных своих сотрудников и клиентов, либо сторонняя организация, уполномоченная компанией-владельцем.

Ответственным субъектам вменяется в обязанность принимать нужные меры для защиты персональных данных от незаконного или просто случайного доступа к ним, удаления, фальсификации, блокировки, несогласованного копирования, размножения персональных данных, а также от других незаконных шагов в отношении личных сведений.

Невыполнение требований мер по обеспечению безопасности при работе с персональными данными предусматривает административную ответственность по статье 13.11 КоАП РФ [2].

Когда обработка происходит с использованием информационных систем, появляются новые потенциальные угрозы, которые нужно свести к минимуму, а лучше и вовсе исключить.

Актуальные угрозы безопасности персональных данных – совокупность условий и факторов, создающих риск нелегального, в том числе случайного доступа к персональным данным в процессе обработки в информационной системе. В ходе этого нарушители могут уничтожать, менять, блокировать, копировать, предоставлять, распространять данные, а также совершать иные неправомерные действия.

Актуальные угрозы информационной системы персональных данных указаны в постановлении Правительства РФ №1119 [3]. В соответствии с этим документом они делятся на три типа.

К угрозам первого типа относятся не декларированные, то есть не задокументированные возможности в системном программном обеспечении – операционная система, сервисные программы, антивирусы.

Ко второму типу относятся не декларированные возможности в прикладном программном обеспечении. Оно бывает общего назначения – система управления базами данных и специального – бухгалтерские программы.

К третьему типу относятся угрозы в системном и программном обеспечениях, несвязанные с предыдущими двумя типами угроз.

Для надлежащей защиты персональных данных необходимо:

- установить актуальные угрозы безопасности при обрабатывании информации в информационных системах персональных данных;
- принять адекватные меры организационного и технического характера;
- применять сертифицированные средства информационной защиты;
- перед вводом в эксплуатацию провести аттестацию информационной системы персональных данных на соответствие защитных систем правовым нормам;
- вести учет машинных носителей персональных данных;
- обнаруживать факты незаконного доступа к этой информации и выполнять соответствующие действия по улучшению их защиты;
- восстанавливать поврежденную информацию;
- установить режим доступа к персональным данным только строго установленных лиц;
- регистрировать все действия, совершаемые при работе с персональных данных [4].

Пункты для защиты от несанкционированного доступа:

- разрешительная система допусков к информационной системе;
- ограничение возможности входа в помещения с техническими средствами обработки персональных данных;
- регистрация действий при работе с персональными данными;
- строгий учет и хранение съемных носителей данных;
- создание резервных копий баз данных и носителей информации;
- использование сертифицированных средств защиты информации.
- защищенные каналы связи;
- нахождение технических средств обработки персональных данных в пределах охраняемой территории;
- борьба с вредоносными программами и вирусами с помощью сертифицированных антивирусных программ и других методов защиты;
- межсетевое экранирование;
- анализ защищенности информационных систем сканерами безопасности;
- ограждение каналов связи от считывания данных;
- использование смарт-карт, электронных замков для правильной идентификации пользователей;
- систематическое испытание межсетевого экрана имитацией атак извне;
- аутентификация дружественных информсистем и обеспечение целостности пересылаемых данных;
- защита среды виртуализации;
- управление конфигурацией информационной системы и системы защиты [4].

Полный перечень технических и организационных мер по обеспечению безопасности также определен юридически. Технические средства защиты в свою очередь имеют отдельную классификацию и должны выбираться в зависимости от требуемого уровня защиты. К ним относятся процедура идентификации и аутентификации субъектов и объектов доступа, цепочка управления доступом, ограничение программной среды, надежная защита машинных носителей информации, антивирусная защита, предотвращение и обнаружение вторжений [5].

Одним из наиболее действенных способов защиты персональных данных является использование средств криптографии – аппаратные, программные и комбинированные устройства и комплексы, способные реализовывать алгоритмы криптографического преобразования информации.

Они предназначены одновременно для защиты информации при передаче по каналам связи и защиты ее от неразрешенного доступа при обработке и хранении. Логика проста: злоумышленник, который не знает кода, не сможет воспользоваться данными, даже если получит к ним доступ, поскольку не прочтет их. Для него они останутся бессмысленным набором как будто случайных цифр.

Если для защиты персональных данных применяются какие-либо криптографические средства, их применение регламентировано приказом ФСБ России № 378 от 10.07.2014 [6].

Несмотря на изрядную запутанность руководящих документов по защите информационных систем, в том числе, хранящих в них данных, соблюсти основные нормы, установленные в этих документах, реально.

В целом, последовательность действий лица, планирующего обработку персональных данных, должна быть примерно следующей:

- определить, относится ли он к категории «оператор персональных данных»;
- если относится, известить о своих планах Роскомнадзор;
- определить угрозы безопасности данных при их обработке в информационной системе оператора;
- определить требующийся уровень защиты;
- определить и применить организационные и технические меры защиты данных от неправомерного доступа к ним, а также от возможной их утраты или искажения;
- применить выбранные меры защиты;
- регистрировать и учитывать все действия, совершаемых с персональными данными в информационной системе;
- обеспечить обнаружение фактов несанкционированного доступа к данным и принимать меры, исключающие такой доступ в дальнейшем;
- регулярно оценивать эффективность применения выбранных средств защиты [7].

Согласно пункту 10 приказа ФСТЭК № 21 от 18.02.2013, при невозможности реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а также с учётом экономической целесообразности могут разрабатываться компенсирующие меры, направленные на нейтрализацию актуальных угроз безопасности данных [8].

В заключении отметим, что необходимо регулярно проводить оценку эффективности выбранных мер защиты и своевременно обновлять их, следить за изменениями в законодательстве. Предупредить угрозу в разы проще и дешевле, чем бороться с ее последствиями.

Список литературы:

1. Федеральный закон № 152-ФЗ «О персональных данных» от 27.07.2006;
2. Кодекс Российской Федерации об административных правонарушениях" № 195-ФЗ (ред. от 25.12.2023) Статья 13.11. Нарушение законодательства Российской Федерации в области персональных данных от 30.12.2001;
3. Постановление Правительства РФ № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012;
4. Электронный ресурс: Особенности защиты персональных данных https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/realizaciya-zashchity-personalnyh-dannyh/osobennosti-zashchity-personalnyh-dannyh/

5. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК) № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013;

6. Приказ ФСБ России № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости» от 10 июля 2014 г.;

7. Электронный ресурс: Персональные данные: средства защиты https://1cloud.ru/blog/personalnye-dannye-chast-2%3Futm_source%3Dhabrahabr%26utm_medium%3Dcpm%26utm_campaign%3Dlinuxbug%26utm_content%3Dblog

8. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006.