Энциклопедия решений. Обеспечение безопасности персональных данных при их обработке в информационных системах (ноябрь 2024)

Обеспечение безопасности персональных данных при их обработке в информационных системах

Смотрите в этом материале:
- оценка эффективности мер по обеспечению безопасности персональных данных;
- использование средств криптографической защиты информации для обеспечения безопасности персональных данных;
- меры по обеспечению безопасности персональных данных

Согласно ч. 1 ст. 19 Закона N 152-ФЗ оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Как следует из ч. 2 ст. 19 Закона N 152-ФЗ, обеспечение безопасности персональных данных в информационных системах достигается, в частности:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности персональных данных;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учетом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Примерный перечень правовых, организационных и технических мер защиты персональных данных приведен в ч. ч. 1, 2 ст. 18.1 Закона N 152-ФЗ.

Особенности защиты персональных данных при автоматизированной обработке детализированы в постановлении Правительства РФ от 01.11.2012 N 1119 (далее - Постановление N 1119).

В п. 2 Постановления N 1119 указано, что безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы. Система такой защиты включает в

себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах. Выбор конкретных средств защиты конфиденциальной информации осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности РФ (ФСБ России) и Федеральной службой по техническому и экспортному контролю (ФСТЭК) во исполнение ч. 4 ст. 19 Закона N 152-ФЗ (п. 4 Постановления N 1119). Такими документами, в частности, являются:

- приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (далее - Приказ ФСТЭК N 21);

- приказ ФСТЭК России от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"*(1);

- приказ ФСБ России от 10.07.2014 N 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 защищенности";

- Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденные приказом ФСТЭК России от 02.06.2020 N 76;

- Методика оценки угроз безопасности информации, утв. ФСТЭК 05.02.2021;

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка), утв. ФСТЭК 15.02.2008

и др.

Подчеркнем, перечисленные документы имеют сугубо технический характер, что требует специальных познаний в сфере информационной безопасности. Поэтому для создания и реализации эффективной системы защиты конфиденциальной информации необходимо привлечение профильных специалистов.

В конечном итоге должна быть спроектирована и введена в эксплуатацию эффективная система защиты персональных данных в информационной системе или приведена в соответствие с требованиями действующего законодательства уже существующая у оператора система.

Меры по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности и применяемых информационных технологий, перечислены в п. 8 Приказа ФСТЭК N 21. Их выбор зависит от уровня защищенности информационной системы и уровня доверия*(2). Всего выделяется четыре уровня защищенности (п. 8 Постановления N 1119), которые сгруппированы в зависимости от категории обрабатываемых персональных данных (общедоступные, специальные биометрические); характера отношений между субъектом и оператором (работники, сторонние лица); количества субъектов, чьи персональные данные обрабатываются (больше или меньше 100 000 человек); типов актуальных угроз безопасности информационной системы*(3) (п. п. 9-12 Постановления N 1119).

Иерархически упорядоченные оценочные уровни доверия (ОУД) для оценки уровня доверия к техническим средствам приведены в п. 7 Национального стандарта РФ ГОСТ Р ИСО/МЭК 15408-3-2013 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности". Их всего семь. Каждый последующий ОУД представляет более высокое доверие, чем любой из предыдущих. Увеличение доверия от предыдущего ОУД к последующему достигается заменой какого-либо компонента доверия иерархичным компонентом из того же семейства доверия (т. е. увеличением строгости, области охвата и/или глубины оценки) и добавлением компонентов из других семейств доверия (т. е. добавлением новых требований).

Выполнение требований к уровню доверия является обязательным при проведении работ по сертификации средств защиты информации, организуемых ФСТЭК России в

пределах своих полномочий.

Оценка эффективности мер по обеспечению безопасности персональных данных

Под оценкой эффективности мер по обеспечению безопасности персональных данных понимается комплекс организационно-технических мероприятий, в результате которых подтверждается, что информационная система персональных данных соответствует установленным требованиям.

Оценка эффективности принимаемых мер проводится оператором (уполномоченным лицом) самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации (п. 17 Постановления № 1119). Форма документа, создаваемого по результатам такой оценки, нормативно не установлена, что позволяет оператору разработать ее самостоятельно (см. также п. 3 Информационного сообщения ФСТЭК России от 15.07.2013 N 240/22/2637*(4)).

Отметим также, что оператор при создании системы безопасности персональных данных должен применять средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия средств защиты информации (п. 3 ч. 2 ст. 19 Закона № 152-ФЗ). Аналогичные требования содержатся в п. 13 Постановления № 1119 и п. 4 Приказа ФСТЭК № 21. При этом в названных нормах не говорится об обязательной сертификации таких средств*(5). На этом основании, мы считаем, что оценка соответствия может быть любой, главное, чтобы проверка соответствия была задокументирована. Иными словами, хозяйствующий субъект в отсутствие обязательных предписаний может использовать и несертифицированные средства защиты.

Использование средств криптографической защиты информации для обеспечения безопасности персональных данных

В п. 6 Приказа ФСТЭК N 21 определено, что для всех уровней защищенности должен быть реализован защищенный удаленный доступ субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети, включая средства криптографической защиты информации (СКЗИ). При этом использование СКЗИ для обеспечения безопасности персональных данных обязательно, если персональные данные подлежат криптографической защите в соответствии с законодательством Российской Федерации, а также если в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ.

К случаям, когда угрозы могут быть нейтрализованы только с помощью СКЗИ, относятся: передача персональных данных по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при передаче персональных данных по информационно-телекоммуникационным сетям общего пользования); хранение персональных данных на носителях информации, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов.

Кроме того, решение о необходимости криптографической защиты персональных данных может быть принято конкретным оператором на основании технико-экономического сравнения альтернативных вариантов обеспечения требуемых характеристик безопасности информации, содержащей, в том числе, персональные данные.

Причем для обеспечения безопасности персональных данных при их автоматизированной обработке должны использоваться только СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия, то есть сертифицированные*(6) (см. Методические рекомендации, утв. ФСБ России 31.03.2015 N 149/7/2/6-432).

Таким образом, хозяйствующим субъектам не обязательно использовать криптографию для обеспечения безопасности персональных данных в информационных системах.

Меры по обеспечению безопасности персональных данных, реализуемых в рамках защиты персональных данных с учетом актуальных угроз безопасности и применяемых информационных технологий

N	Перечень мер	Цель реализации
1	идентификация и аутентификация субъектов доступа и объектов доступа	обеспечение присвоения субъектам и объектам доступа уникального признака (идентификатора), сравнения предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверка принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности)
2	управление доступом субъектов доступа к объектам доступа	обеспечение управления правами и привилегиями субъектов доступа, разграничения доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также контроля за соблюдением этих правил
3	ограничение программной среды	обеспечение установки и (или) запуска только разрешенного к использованию в информационной системе программного обеспечения или исключение возможности установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения
4	защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные	исключение возможности несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированного использования съемных машинных носителей персональных данных
5	регистрация событий безопасности	обеспечение сбора, записи, хранения и защиты информации о событиях безопасности в информационной системе, а также возможности просмотра и анализа информации о таких событиях и реагирования на них
6	антивирусная защита	обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации
7	обнаружение (предотвращение) вторжений	обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия
8	контроль (анализ) защищенности персональных данных	обеспечение контроля уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и

		тестированию работоспособности системы защиты персональных данных
9	обеспечение целостности информационной системы и персональных данных	обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных
10	обеспечение доступности персональных данных	авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы
11	защита среды виртуализации	исключение несанкционированного доступа к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействия на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям
12	защита технических средств	Исключение несанкционированного доступа к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы, и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей
13	защита информационной системы, ее средств, систем связи и передачи данных	обеспечение защиты персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных
14	выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них	обеспечение обнаружения, идентификации, анализа инцидентов в информационной системе, а также принятия мер по устранению и предупреждению инцидентов

15	управление конфигурацией информационной системы и системы защиты персональных данных	обеспечение управления изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирования этих изменений

---

*(1) Несмотря на то, что данный документ адресован операторам, обрабатывающим персональные данные в государственных информационных системах, он в полной мере может использоваться и для построения системы защиты информации ограниченного доступа юридическими лицами негосударственного сектора (п. 6 Приказа)

*(2) Уровни доверия устанавливаются в соответствии с Требованиями по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденные приказом ФСТЭК России от 02.06.2020 N 76.

*(3) Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия. Всего выделяется три типа таких угроз (п. 6 Постановления N 1119)

*(4) Размещен на сайте ФСТЭК: https://fstec.ru/index?id=716:informatsionnoe-soobshchenie-fstek-rossii-1

*(5) Например, в п. 11 Приказа ФСТЭК N 17 прямо указано, что для обеспечения защиты информации, содержащейся в государственной информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со ст. 5 Федерального закона от 27.12.2002 N 184-ФЗ "О техническом регулировании". См. Извещение ФСБ России от 18.07.2016.

*(6) Перечень СКЗИ, сертифицированных ФСБ России, опубликован на официальном сайте Центра по лицензированию, сертификации и защите государственной тайны ФСБ России (http://clsz.fsb.ru/).