***Эссе***

По результатам анализа нормативных документов о персональных данных и информационных системах предоставляется субъективный обзор данной документации.

Сначала рассмотрим требования к жизненному циклу государственных информационных систем (далее - ГИС) (**Постановление № 676**)

Относительно данных в ГИС должно быть обеспечено:

а) требования о защите информации, содержащейся в системах, устанавливаемые федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий;

б) требования к организации и мерам защиты информации, содержащейся в системе;

в) требования о защите персональных данных, предусмотренные [частью 3 статьи 19](https://base.garant.ru/12148567/95ef042b11da42ac166eeedeb998f688/#block_1903) Федерального закона "О персональных данных" (в случае наличия в системе персональных данных);

г) требования к обеспечению доступа к информации, содержащейся в системе, органам местного самоуправления и органам публичной власти федеральных территорий в необходимых случаях для обеспечения ее обработки посредством информационных технологий и технических средств, входящих в состав системы.

В целях защиты информации в ГИС уполномоченные государственные органы реализуют:

а) определение информации, подлежащей защите от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации;

б) анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать система;

в) классификацию системы в соответствии с требованиями о защите информации;

г) определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в системе, и разработку на их основе модели угроз безопасности информации;

д) определение требований к информационной системе (подсистеме) защиты информации, содержащейся в системе.

Также должен вестись учет ИТ-активов уполномоченными государственными органами.

Основанием для создания ГИС является:

а) обязанность государственного органа по созданию системы, предусмотренная нормативными правовыми актами;

а1) обязанность уполномоченной организации по созданию системы, предусмотренная федеральным законом;

б) решение государственного органа о создании системы с целью обеспечения реализации возложенных на него полномочий;

в) решение Правительства Российской Федерации о реализации проекта государственно-частного партнерства;

г) решение высшего исполнительного органа субъекта Российской Федерации о реализации проекта государственно-частного партнерства, если публичным партнером является субъект Российской Федерации либо планируется проведение совместного конкурса с участием субъекта Российской Федерации (за исключением случаев проведения совместного конкурса с участием Российской Федерации);

д) решение Правительства Российской Федерации о заключении концессионного соглашения;

е) решение высшего исполнительного органа субъекта Российской Федерации о заключении концессионного соглашения, если концедентом является субъект Российской Федерации.

ГИС должна иметь технико-экономическое обоснование реализации системы. Концепция является документом технической документации на систему и содержит обоснование вариантов построения системы, условия и мероприятия по ее созданию, на основе которых принимается решение о необходимости и целесообразности создания системы, формируются требования к ней, а также обеспечиваются единый контекст и взаимосвязь результатов реализации требований к системе на последующих этапах ее жизненного цикла, в том числе при разработке технического задания на систему. В концепции приводятся в том числе:

а) результаты анализа нормативных правовых актов, методических документов, международных и национальных стандартов Российской Федерации, в соответствии с которыми разрабатывается система;

б) классификация системы в соответствии с требованиями о защите информации;

в) описание выявленных проблем, решение которых возможно средствами системы, описание требований к системе, включая определение требований к информационной системе (подсистеме) защиты информации и допустимых затрат на разработку, ввод в действие и эксплуатацию системы, описание эффекта, ожидаемого от создания системы, условий создания и функционирования системы, а также описание автоматизируемых процессов деятельности (как существующих, так и планируемых к реализации посредством создания системы) и архитектуры системы;

г) цели и задачи создания системы, архитектура системы, включая состав, выполняемые функции и взаимосвязи компонентов системы, состав сведений, подлежащих размещению в системе, обоснование выбранного варианта построения системы;

д) показатели степени автоматизации процессов и их значений, которые должны быть достигнуты в результате создания системы, а также критерии оценки достижения целей создания системы;

е) оценка финансовых, трудовых и материальных ресурсов, необходимых для реализации требований, указанных в [подпункте "в"](https://base.garant.ru/71120998/f71146013d8ca605bb28a6980a188d6d/#block_10213) настоящего пункта (технико-экономическое обоснование), включая оценку указанных ресурсов для создания системы, ввода ее в эксплуатацию, эксплуатации и в случае, если установлен срок эксплуатации системы, оценку необходимых ресурсов для вывода системы из эксплуатации и дальнейшего хранения содержащейся в ее базах данных информации;

ж) способ создания системы - последовательный или с применением итерационного подхода к разработке системы.

Создание системы допускается осуществлять очередями. В этом случае концепция создания системы должна включать в себя описание всех очередей системы, техническое задание разрабатывается на каждую очередь системы.

Порядок создания системы включает следующие этапы:

а) разработка документации на систему и ее части;

б) разработка или адаптация программного обеспечения, разработка рабочей документации;

г) пусконаладочные работы;

д) проведение предварительных испытаний системы;

е) проведение опытной эксплуатации системы;

ж) проведение приемочных испытаний системы.

Техническая и методическая документация, разрабатываемая на соответствующих этапах жизненного цикла системы, в том числе концепция и техническое задание на создание системы (очереди системы), документация, разрабатываемая на этапах создания ГИС, а также программы для электронных вычислительных машин (включая тексты указанных программ и дистрибутивы, клиентское программное обеспечение системы и использованное свободное программное обеспечение), сведения о программных интерфейсах системы, алгоритмы, электронные модели автоматизируемых процессов деятельности, архитектуры системы и базы данных системы, использованные при создании (развитии) системы, подлежат размещению и публикации в национальном фонде алгоритмов и программ для электронных вычислительных машин в соответствии с требованиями настоящего документа и требованиями, установленными [Положением](https://base.garant.ru/70308380/fe2a8f253d3803b2aa636e7d143cb80b/#block_1000) о национальном фонде алгоритмов и программ.

Основанием для вывода системы из эксплуатации является:

а) завершение срока эксплуатации системы, в случае если такой срок был установлен нормативным правовым актом;

б) нецелесообразность эксплуатации системы, в том числе низкая эффективность используемых технических средств и программного обеспечения, изменение правового регулирования, принятие управленческих решений, а также наличие иных изменений, препятствующих эксплуатации системы;

в) финансово-экономическая неэффективность эксплуатации системы.

Вывод системы из эксплуатации происходит правовым актом уполномоченного государственного органа при наличии одного или нескольких оснований.

Правовой акт о выводе системы из эксплуатации включает:

а) основание для вывода системы из эксплуатации;

б) перечень и сроки реализации мероприятий по выводу системы из эксплуатации;

в) порядок, сроки, режим хранения и дальнейшего использования информационных ресурсов, включая порядок обеспечения доступа к информационным ресурсам выводимой из эксплуатации системы и обеспечения защиты информации, содержащейся в выводимой из эксплуатации системе;

г) порядок, сроки и способы информирования пользователей о выводе системы из эксплуатации.

Перечень мероприятий по выводу системы из эксплуатации включает:

а) подготовку правовых актов, связанных с выводом системы из эксплуатации;

б) работы по выводу системы из эксплуатации, в том числе работы по деинсталляции программного обеспечения системы, по реализации прав на программное обеспечение системы, демонтажу и списанию технических средств системы, обеспечению хранения и дальнейшего использования информационных ресурсов системы;

в) обеспечение защиты информации в соответствии с документацией на систему и организационно-распорядительными документами по защите информации, в том числе архивирование информации, содержащейся в системе, уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

Если нормативными правовыми актами Российской Федерации не установлено иное, то сроки хранения информации, содержащейся в базах данных системы, определяются государственным органом, и не могут быть меньше сроков хранения информации, которые установлены для хранения документов в бумажном виде, содержащих такую информацию.

Срок вывода системы из эксплуатации не может быть ранее срока окончания последнего мероприятия, предусмотренного правовым актом о выводе системы из эксплуатации.

Меры по обеспечению безопаности персональных данных описаны в **ФСТЭК 21.**

В данные меры входят:

1. идентификация и аутентификация субъектов доступа и объектов доступа;
2. управление доступом субъектов доступа к объектам доступа;
3. ограничение программной среды;
4. защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее – машинные носители персональных данных);
5. регистрация событий безопасности;
6. антивирусная защита;
7. обнаружение (предотвращение) вторжений;
8. контроль (анализ) защищенности персональных данных;
9. обеспечение целостности информационной системы и персональных данных;
10. обеспечение доступности персональных данных;
11. защита среды виртуализации;
12. защита технических средств;
13. защита информационной системы, ее средств, систем связи и передачи 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;
15. управление конфигурацией информационной системы и системы защиты персональных данных.

При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а также с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных.

В этом случае в ходе разработки системы защиты персональных данных должно быть проведено обоснование применения компенсирующих мер для обеспечения безопасности персональных данных.

В случае определения в соответствии с Требованиями к защите персональных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119, в качестве актуальных угроз безопасности персональных данных 1-го и 2-го типов дополнительно к мерам по обеспечению безопасности персональных данных, могут применяться следующие меры:

* проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей с использованием автоматизированных средств и (или) без использования таковых;
* тестирование информационной системы на проникновения;
* использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.

Что касается обеспечения безопасности персональных данных при их обработке, данный аспект регулирует **Федеральный закон №152 Статья 19**.

Обеспечение безопасности персональных данных при обработке персональных данных достигается в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) 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 Российской Федерации [уровни защищенности](https://base.garant.ru/70252506/f40a9f9fc2260e303cddfef5d7575dce/#block_10) персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

3.1) применением для уничтожения персональных данных, прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, в составе которых реализована функция уничтожения информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) 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;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) 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;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Оператор обязан обрабатывать персональные данные сотрудников органов федеральной службы безопасности, лиц, оказывающих или оказывавших им содействие на конфиденциальной основе, подлежащих государственной защите судей, должностных лиц правоохранительных и контролирующих органов, сотрудников органов внешней разведки Российской Федерации, лиц, оказывающих или оказывавших им содействие на конфиденциальной основе, объектов государственной охраны и членов их семей, сотрудников органов государственной охраны, лиц, оказывающих или оказывавших им содействие на конфиденциальной основе, подлежащих государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства, сотрудников органов внутренних дел, лиц, оказывающих или оказывавших им содействие на конфиденциальной основе.

***Основные определения на английском языке:***

1. [Personal Data](https://www.google.com/search?sca_esv=0f9b108d57af51d0&cs=0&sxsrf=AE3TifO92JtgNQC2x6ZLa60WUAYFKVUPmA%3A1756848411167&q=Personal+Data&sa=X&ved=2ahUKEwjL68irgruPAxU8JxAIHWNUMVoQxccNegQICxAB&mstk=AUtExfDe-5aONkbNQcBhvs-ft_rReNLg5vX53knVtNamFozDLNnXt1EMUwwN99h28JDn2kr3NPEJyXnyfcH7jgvFuil9y82hIsnt2MQfZGtnRckqCvTICNXllTZ9mg4aittAS0LoyYtvnPBzDDbgdM7fZvep3JxQ6mW1-p-OowJeVFN3n1uHQYaHi1b48IiZUVOrHFWcEcvsgT6KfM62udvouHFQFLxrSQJaSLeqlrHmbTW8Mh7tuv9HQTRuYrmB_dCFStqY3rjclDKsCrNxr06XjuoH&csui=3) **– персональные данные;**
2. **Data Subject Rights** — права субъекта данных;
3. DSR Request — официальный запрос субъекта данных контроллеру с целью совершения какого-либо действия над его или ее персональными данными;
4. DPO (Data Protection Officer) — сотрудник по защите данных и взаимодействия с субъектами данных и надзорными органами;
5. **Controller -** физическое или юридическое лицо, орган государственной власти, агентство или другой орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных;
6. **Processor –** физическое или юридическое лицо, орган государственной власти, агентство или другой орган, который обрабатывает персональные данные от имени контролера;
7. **Processing –** любая операция или набор операций, выполняемых с персональными данными или наборами персональных данных;
8. **Consent** – любое добровольное, конкретное, информированное и недвусмысленное указание на пожелания субъекта данных, посредством заявления или ясного утвердительного действия, которым субъект данных дает согласие на обработку персональных данных, относящихся к нему;
9. Privacy by design – спроектированная защита данных (защита встраивается на самых ранних этапах);
10. Privacy by default – защита конфиденциальности пользователя по умолчанию.

***Аналогичные иностранные стандарты:***

***ISO/IEC 27001 (the International Organization for Standardization) and IEC (the International Electrotechnical Commission)*** определяет требования к Системе Менеджмента Информационной Безопасности (СМИБ), предоставляя структурированный подход к управлению рисками, защите конфиденциальных данных и постоянному совершенствованию безопасности.

В Приложении A представлен набор мер по обеспечению информационной безопасности, которые организации могут использовать для защиты своих активов. Эти контроллеры группируются по категориям, таким как организационные, персонала, физические и технологические, и служат основой для разработки собственной, более детальной политики безопасности

***GDPR (General Data Protection Regulation)***

**Основные принципы:**

1. Принцип законности, справедливости и прозрачности. Персональные данные должны быть получены законными и справедливыми средствами с согласия субъекта данных;
2. Ограничение цели. Цель сбора данных должна быть указана во время сбора, и данные не должны использоваться ни для чего иного, кроме первоначального намерения;
3. Минимизация данных. Собранные данные должны соответствовать заданной изначально цели. Запрещается собирать данные в большем объеме, чем это требуется для достижения цели;
4. Точность. Персональная информация должна быть точной, полной и актуальной, насколько это необходимо для заданных целей. Если такие данные будут считаться неточными, они должны быть стерты или исправлены (по запросу пользователя);
5. Ограничение хранения. Данные хранятся в форме, которая позволяет идентифицировать пользователя не дольше, чем это необходимо для выполнения целей обработки информации;
6. Целостность и конфиденциальность. Личные данные должны быть защищены гарантиями безопасности от таких рисков, как потеря или несанкционированный доступ, уничтожение, использование, модификация или раскрытие данных;
7. Подотчетность. Контролер несет ответственность и должен быть готов продемонстрировать соблюдение мер, указанных выше.

[***Директива о конфиденциальности в сфере электронных коммуникаций (ePrivacy Directive)***](https://www.google.com/search?sca_esv=0f9b108d57af51d0&cs=0&sxsrf=AE3TifN68FpOmD4EGpBrJaT4s8db2130JQ%3A1756850456890&q=%D0%94%D0%B8%D1%80%D0%B5%D0%BA%D1%82%D0%B8%D0%B2%D1%8B+%D0%BE+%D0%BA%D0%BE%D0%BD%D1%84%D0%B8%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D0%B8+%D0%B2+%D1%81%D1%84%D0%B5%D1%80%D0%B5+%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D1%85+%D0%BA%D0%BE%D0%BC%D0%BC%D1%83%D0%BD%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%B9+%28ePrivacy+Directive%29&sa=X&ved=2ahUKEwi92Ib7ibuPAxW9FxAIHYy8MKQQxccNegQIAhAB&mstk=AUtExfDbErcKanCg1hwD-JWETzsMws150nKJvU2zkrKdfuvyk_WUalROgj3hwuWyuSdyyHNmXf0IDZfl73RpZx48MA0JqjCMjDlYGVuY4M7PyC7H5E0BYahYdKYnhhPgOKi24qwqGPfgIXGgPKn3I99rDlx-jzOGh7X65CU7PiMtkk5nCe0_qnNFM0ZXpLTve4jaVl2iG97BfUjk-4JKq3qmGQcjFC2FgUFJn9LFHNG7aaxFjcRYjMgakzezBLeaOgSVzf-MEttjclP_W23KEuE3ldvv&csui=3)***(Директива 2002/58/ЕС)*** обязует получать согласие пользователей на сохранение файлов cookie, кроме строго необходимых случаев, а также информировать пользователей о назначении cookie до получения их согласия. Директива распространяется на сектор электронных коммуникаций и требует гарантий конфиденциальности сообщений и данных о трафике.