

Whitepaper

Примерный алгоритм действий, направленных на
выполнение требований
№152-ФЗ «О персональных данных»

При выполнении работ по приведению процессов обработки персональных данных в организации к соответствию требованиям №152-ФЗ необходимо:

1. Провести аудит процессов обработки персональных данных в организации, в рамках аудита:

1.1. Выяснить организационную структуру (штатное расписание, наличие структурных подразделений ИТ и ИБ, наличие ДЗР (Департамент по защите активов или иное наименование должности, предусматривающей аналогичный функционал)

1.2. Разработать опросный лист для организации, направить в организацию для заполнения анкету (опросный лист), содержащий вопросы, касающиеся бизнес-процессов в рамках обработки ПДн.

1.3. Изучить действующие документы по информационной безопасности (инструкции, регламенты, приказы и т.д.), регламентирующие обработку ПДн и иной конфиденциальной информации.

1.4. Проанализировать ИТ-инфраструктуру Заказчика (например, методом опроса сотрудников ИТ-подразделений Заказчика) в части обеспечения ИБ и общей архитектуры, выявить количество рабочих станций, серверов, виртуальных машин, средств защиты информации (как сертифицированных ФСТЭК России, так и несертифицированных), используемого системного прикладного и системного ПО и т.д.

1.5. По итогу анализа анкет, заполненных руководителями структурных подразделений, сопоставить данные, полученные в ходе анализа ИТ-инфраструктуры, приступить к следующему этапу *(когда каждый руководитель СП заполняет сведения, относительно процессов обрабатываемой информации ограниченного доступа, такой метод наиболее достоверно отражает фактическое состояние процессов обработки конфиденциальной информации)*

2. На данном этапе мы получили заполненный опросный лист от организации Заказчика, полученные сведения должны содержать информацию:

- тип (локальный, распределенный и т.д.), размер и состав ИТ-инфраструктуры, участвующей в процессах обработки ПДн и конфиденциальной информации;

- перечень категорий обрабатываемых персональных данных (биометрические, специальные, иные, общедоступные);

- категории субъектов персональных данных (работники, не работники, контрагенты, совершеннолетние/несовершеннолетние, родственники работников и соискателей, соискатели, и т.д.);

- перечень действий, совершаемых с персональными данными (**статья 3 №152-ФЗ**);

- правовые основания обработки персональных данных (**статья 6 №152-ФЗ, согласие субъекта или иное условие, указанное в статье**);

- срок обработки ПДн (регламентируется согласием субъекта, требованиями законодательства РФ (в случае, если ПДн обрабатываются на основании Федерального закона, когда согласие субъекта не обязательно), целями обработки;

- количество субъектов ПДн, данные которых обрабатываются (также следует учитывать данные, хранящиеся в резервных хранилищах (бэкапах);

- сотрудники и структурные подразделения Заказчика, участвующие в обработке;

- наличие материальных носителей ПДн (электронные и бумажные), перечень мест их хранения;

- наличие процессов передачи персональных данных третьим лицам и трансграничной передачи, правовые основания такой передачи персональных данных;

- используемые информационные системы персональных данных (ИСПДн), например: «1С», «Почтовый сервер», «Файловый сервер», «Справочник» (ActiveDirectory);

- способ осуществления контроля доступа (договор с охранной организацией, СКУД, охрану обеспечивает собственник (в случае аренды и охраны со стороны собственника), и т.д.;

- иные сведения, которые могут иметь значение для проекта, пример опросного листа будет в приложении.

3. Чтобы не усложнять процесс, во избежание лишних трудностей, в том числе у Заказчика, подробные сведения об ИТ-инфраструктуре и архитектуре ИСПДн лучше вывести в отдельные опросные листы, применимые к каждой ИСПДн, указанной сотрудниками Заказчика.

- используемое ПО (системное, прикладное и т.д.);

- наличие и перечень средств защиты информации;

- перечень сетевого/коммутационного оборудования;

- наличие и перечень используемых средств криптографической защиты (СКЗИ), в том числе средств электронной подписи (ЭП);

- способы обработки персональных данных (автоматизированный и неавтоматизированный);

- какими структурными подразделениями или работниками осуществляется администрирование/разработка/доработка/поддержка, или внешними подрядчиками;

- перечень лиц/должностей, имеющих непосредственный доступ к ИСПДн в части обработки персональных данных (в том числе просмотр);

- категории субъектов и персональных данных, обрабатываемых в системе (ИСПДн);

- состав полей для ПДн внутри ИС, а также источники персональных данных (откуда данные заносят и какие, кому принадлежат данные (работникам/соискателям/иным субъектам);
- архитектурная схема ИСПДн (также может включать сведения о взаимодействии с сетевым/коммутационным оборудованием, СЗИ, СКЗИ и т.д.);
- данные о взаимодействии ИСПДн с внешними и внутренними системами;
- данные о сетевых адресах/именах, а также расположении хостов (физическом), в составе ИСПДн.

Какие требования выполняются?

По состоянию на сегодняшний день, требования к организации процессов обработки персональных данных регламентируются множеством документов, также существует большое количество методических и руководящих документов ФСТЭК России <https://fstec.ru/dokumenty-filter> (например методика по разработке модели угроз, методика по управлению уязвимостями, и т.д.), которые могут не являться обязательными к исполнению, но выполнение рекомендаций и указаний в таких документах позитивно влияет на ситуацию при осуществлении проверок со стороны регулирующих органов (в частности РКН).

В зависимости от организационно-правовой формы и принадлежности организации к определенной сфере деятельности будет определяться перечень применимых требований по организации процессов обработки ПДн и защите этих данных. Например, финансовые организации в части требований по защите персональных данных руководствуются требованиями Центрального Банка РФ (ГОСТ 57580 «Защита финансовых организаций» <https://docs.cntd.ru/document/1200146534> и иные), государственные и бюджетные учреждения также могут быть обязаны выполнять конкретные требования Федеральных органов власти, уполномоченных разрабатывать требования ИБ (например, для ЖД-вокзала будут более актуальными требования Министерства транспорта РФ и т.д., при наличии таких требований).

Если касаться вопросов требований, применимых к «типовой» коммерческой организации, осуществляющей деятельность в какой-либо сфере (продажа товаров, оказание услуг), то основными документами, которыми следует руководствоваться при работе с требованиями будут:

- №152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (ПП №1119);
- Приказ ФСТЭК России от 18 февраля 2013 г. N 21;

- Приказ ФСБ России от 10 июля 2014 г. N 378 (применяется при наличии в инфраструктуре СКЗИ, предназначенных для защиты ПДн, например – удаленный доступ с использованием VPN-соединения);

- Постановление Правительства РФ от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (само по себе, похоже на почти готовый регламент обработки ПДн с использованием неавтоматизированных (ручных) способов обработки, необходимо применить при наличии «бумажного» документооборота в сфере обработки ПДн);

Вышеуказанный, выделенный перечень, является основным для «типовой» коммерческой организации, он не исчерпывающий, по состоянию на 2024 год также требуется проводить оценку вреда, который может быть причинен субъекту персональных данных (**подпункт 5, части 1, статьи 18.1. №152-ФЗ, ссылка в «закрытом» доступе консультанта +**).

Рекомендуется регулярно перед выполнением работ проверять актуальность ссылок, требований и вообще любых документов, с которыми предстоит работать.

Если более детально рассмотреть 3 документа (**№152-ФЗ, №1119 ПП, ФСТЭК №21**), то последовательно можно определить действия, которые необходимо выполнить в рамках №152-ФЗ. Если кратко, то №152-ФЗ описывает общие требования к принципам, условиям обработки ПДн, права и обязанности Оператора и Субъекта ПДн, и т.д., **№1119 ПП** – нужно для категорирования ИСПДн, в зависимости от параметров присваивается уровень защищенности каждой ИСПДн, также указаны некоторые обязательные организационные требования, которые должны быть применены в ИСПДн исходя из присвоенного уровня защищенности.

После определения уровня защищенности ИСПДн можно приступить к требованиям Приказа **№21 ФСТЭК** России, который уже детально раскрывает нюансы технических мер, попробуем проверить вышеизложенное на практике:

1. Согласно **статье 5 №152-ФЗ** необходимо убедиться, что все обрабатываемые персональные данные обрабатываются в соответствии с целями их обработки. Например, если обрабатываются персональные данные клиента, которые заносятся клиентом на сайте в специальной форме, с целью дальнейшей продажи товара или услуги, информация о которой размещена на сайте, то в таком случае сбор сведений о дате рождения пользователя может быть избыточным (если у товара отсутствуют возрастные ограничения). По итогу аудита процессов обработки ПДн, избыточные данные, не отвечающие целям обработки, должны быть исключены из процесса.

2. В соответствии **со статьей 6 №152-ФЗ** (Условия обработки персональных данных), необходимо убедиться, что все перечисленные в анкетах данные обрабатываются на законных основаниях. Законным основанием обработки может являться согласие субъекта персональных

данных или иное основание, указанное в **части 1 статьи 6 №152-ФЗ**, например **подпунктом 2 части 1 статьи 6** предусмотрено, что персональные данные могут обрабатываться на основании требований иных ФЗ, без согласия субъекта. Однако, если по какой-то причине есть сомнения в необходимости согласия, законом не запрещено брать согласие субъекта в тех случаях, когда отсутствует такая необходимость. Если субъектом дано согласие на обработку, которое в дальнейшем было отозвано, требования Федерального закона будут вышестоящими и Оператору необходимо будет их исполнять, несмотря на волеизъявление субъекта.

3. **Статья 7 №152-ФЗ** предусматривает, что передача ПДн третьим лицам без согласия субъекта запрещена, если **иное не предусмотрено федеральным законом (возвращаясь к пункту выше)**

4. **Статья 8 №152-ФЗ** предусматривает, что в целях информационного обеспечения могут создаваться общедоступные источники персональных данных, на мой взгляд, в данной статье говорится о ситуациях, когда в рамках организации создаются телефонные и иные справочники сотрудников и размещаются на сайте компании. Здесь важно учесть, что при наличии справочников в «закрытом» сегменте корпоративного сайта или БД, при наличии доступа к справочнику только у сотрудников организации, это будет также считаться передачей ПДн и согласие на включение в такой справочник должно быть взято у сотрудника при трудоустройстве (либо включение пункта в общее согласие на обработку ПДн при трудоустройстве).

Если аналогичный справочник размещается в открытом доступе (для всех пользователей интернета), то данная ситуация уже будет квалифицирована как распространение персональных данных неопределенному кругу лиц, что регламентируется **статьей 10.1 №152-ФЗ**, которая была введена в действие относительно недавно, не ранее 2022 года. Исключением будет являться раскрытие ПДн на основании ФЗ о раскрытии информации (налоговые декларации гос.служащих, руководители бюджетных учреждений, и т.д.).

Вывод: если данные размещены на сайте компании, выяснить: 1) кому доступны эти данные? 2) если доступны не только сотрудникам, то есть ли согласие субъектов на передачу? 3) если доступны вообще всем (открытый доступ), имеются ли согласия на распространение ПДн неопределенному кругу лиц? 4) если доступны только сотрудникам и внутри закрытого сегмента, проверить содержание согласия на обработку, на предмет наличия пункта о включении ПДн субъектов в общедоступный рабочий справочник (передача ПДн сотрудникам юр.лица – работодателя).

5. На основании **статьи 9 №152-ФЗ**, следует отметить несколько важных моментов, а именно:

- согласие на обработку ПДн может быть получено в любой доступной форме, позволяющей подтвердить факт его получения;

- согласие должно быть конкретным, предметным, сознательным и однозначным;

- обязанность доказать наличие согласия субъекта возлагается на Оператора (например, при возникновении спорных ситуаций);

- письменное согласие нужно только тогда, когда оно прямо предусмотрено ФЗ (например, сбор биометрических ПДн или согласие на распространение ПДн неопределенному кругу лиц), при этом письменное согласие по своему содержанию должно отвечать требованиям, изложенным в части 4 статьи 9 №152-ФЗ. Согласие также может быть в электронном виде, если подписано УКЭП субъекта (как вариант).

6. **Статья 10 №152-ФЗ** раскрывает, что такое Специальная категория персональных данных и при каких условиях допустима обработка таких данных (касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни). На практике, иногда встречаются случаи, когда в анкете соискателя по какой-то причине оставляют графу «национальность», помимо нарушения Конституции РФ, обработка таких данных без **письменного согласия (ст.9 №152-ФЗ) – недопустима.**

7. **Согласно статье 10.1 №152-ФЗ** (Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения), согласие субъекта персональных данных на распространение **оформляется отдельно от иных согласий и с учётом требований статьи 10.1 №152-ФЗ.** Рекомендуется при наличии таких процессов (раскрытие информации), тщательно проверять содержание таких согласий, наличие отдельной формы, запретов и условий, предусмотренных указанной статьей закона.

8. **Статья 11 №152-ФЗ** раскрывает понятие Биометрических персональных данных, такие данные могут обрабатываться **только при наличии письменного согласия субъекта.** При наличии аудита процессов, следует обратить особое внимание на порядок осуществления допуска на территорию (СКУД), если СКУД использует отпечаток пальца или идет какая-либо автоматизированная сверка по фотографическому изображению, на основании которой принимается решение о пропуске, то в таком случае (когда данные используются для установления личности), с высокой долей вероятности, обрабатываемые ПДн могут быть квалифицированы как «биометрические». Следует избегать обработки Специальной и Биометрической категории персональных данных, так как данные категории наиболее существенно влияют на определение требуемого уровня защищенности согласно **ПП №1119.**

9. **Статья 12 №152-ФЗ** раскрывает понятие «Трансграничная передача» ПДн, если за пределы РФ данные не передаются, то не является актуальным в большинстве случаев. Организации, работающие за рубежом, также учитывают помимо требований данной статьи, нормы «местного»

законодательства, если филиалы и подразделения, а также элементы технической инфраструктуры (БД) размещены на территории другого государства.

10. **Статья 13 №152-ФЗ** описывает особенности обработки ПДн в государственных ИС, которые применимы к владельцам таких ИС. Если осуществляется передача персональных данных сотрудников на основании требований Федерального закона посредством веб-интерфейса ГИС (Госуслуги), то это будет внешняя система по отношению к оператору, а не внутренняя ИСПДн, однако если функция передачи таких сведений осуществляется конкретным сотрудником/структурным подразделением, то АРМ и иное оборудование, участвующее в передаче сведений, и посредством которого осуществляется локальное хранение передаваемых данных, допустимо оформить в виде ИСПДн.

11. **Глава 3 (статьи 14-17 №152-ФЗ)** описывает права субъекта ПДн, рекомендуется ознакомиться самостоятельно. Субъект, в случае нарушения его прав, может взаимодействовать с Оператором через РКН или в судебном порядке, сведения о нарушении прав субъектов также могут стать основанием для инициирования внеплановой проверки Оператора со стороны РКН.

12. **Статья 18 №152-ФЗ** предусматривает обязанности Оператора ПДн по отношению к субъекту, а также условия, при которых Оператор освобождается от обязанности по предоставлению данных субъекту, рекомендуется ознакомиться самостоятельно. Соблюдение требований в отношении прав субъекта обычно включает в себя различные формы обращений по вопросам обработки ПДн субъектов (журнал учёта обращений, форма отзыва, форма согласия, иное).

13. **Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных №152-ФЗ, которые прямо указаны в статье 18.1:**

- **назначение лица, ответственного за организацию обработки персональных данных** (согласно рекомендациям РКН, следует назначать сотрудника – уровня «заместителя руководителя» и т.д., чтобы он имел реальные административные полномочия при организации такой обработки, ограничения, требования или запреты по назначению лица – отсутствуют, назначить можно любого сотрудника;

- **разработать Политику обработки персональных данных** (может называться иначе, главное содержание документа и его суть), подпунктом 2 части 1 статьи 18.1 определяются требования к содержанию документа, также возможно ознакомиться с методическими рекомендациями РКН (ссылок не оставляю, искать актуальные в поисковике, рекомендации также актуализируются со временем). Следует отметить, что форма и структура Политики не определена законом, есть требования по содержанию, общий формат, наименование, структура документа – по желанию Заказчика с

учётом требований вышеуказанного подпункта. Необходимо обеспечить неограниченный доступ к Политике, разместить материальную версию на стенде в офисе организации, разместить на сайте, при наличии процессов сбора ПДн посредством сайта – размещение в открытом доступе обязательно;

- **применение правовых, организационных и технических мер** по обеспечению безопасности персональных данных **в соответствии со статьей 19 №152-ФЗ** (рассмотрим далее);

- **осуществление внутреннего контроля (аудита)** на соответствие требованиям (в законе приводится ссылка на ПП №1119 и Приказ ФСТЭК №17 (ГИСы), что на мой взгляд, буквально означает проведение внутреннего контроля на предмет выполнения требований ПП №1119. Приказ ФСТЭК №17, применимый к ГИС, не относится к ИСПДн (вне ГИС), полагаю целесообразно проводить внутренний контроль на соответствие требованиям ПП №1119 и ФСТЭК №21;

- **провести оценку вреда по требованиям Приказа РКН от 27.10.2022 №178** (приказ небольшой, изучить самостоятельно, обычно, представляет из себя шаблон Приказа о проведении такой оценки и соответствующий акт);

- **ознакомление сотрудников, осуществляющих обработку персональных данных**, с положениями законодательства РФ в сфере обработки ПДн и соответствующих требований, а также с внутренними документами по обработке ПДн. **Чрезвычайно важно** ознакомить сотрудников с наличием документального подтверждения об ознакомлении (лист ознакомления, ЭДО и т.д.). Как правило, при ознакомлении с Политикой обработки, также ставят «галочку» и подпись, что ознакомлены с положениями законодательства РФ в сфере ПДн.

14. **Статья 19 №152-ФЗ**, это та самая статья, которая прямо перечисляет некоторые технические меры, которые должны быть применены (например: учёт машинных носителей ПДн), а также ссылается на **ПП №1119 и ФСТЭК №21**.

15. **Статья 19** также содержит ссылки на иные, отдельные Приказы, например: **Постановление Правительства РФ от 06 июля 2008 года №512** «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных». Исходя из названия документа, можно сделать вывод, что данное Постановление применимо в ситуациях, когда обрабатывается биометрическая категория персональных данных, при этом хранение осуществляется на материальных носителях, требования к которым указаны в Постановлении.

16. Часть 3 **Статьи 19 №152-ФЗ** содержит ссылки на ПП №1119 в части определения уровней защищенности ИСПДн и требований к защите персональных данных при их обработке в ИСПДн, а также ссылки на Приказы

ФСТЭК №21 и ФСБ №378 (при использовании СКЗИ для защиты ПДн) в **Части 4 Статьи 19 №152-ФЗ**.

17. Часть 12-14 **Статьи 19 №152-ФЗ** содержит сведения о необходимости выполнения требований по информированию Операторами ПДн – ФСБ России, в случае инцидентов с персональными данными. Также содержатся ссылки на порядок взаимодействия с НКЦКИ (госсопка) – при необходимости такого взаимодействия.

18. **Статьи 20 и 21** определяют обязанности Оператора при взаимодействии с субъектом ПДн, РКН, представителем субъекта, а также обязанности по устранению нарушений, допущенных при обработке ПДн (например: внесли ошибочные данные, субъект просит их уточнить и изменить на корректные).

19. **Статья 22 №152-ФЗ** содержит обязанность Оператора по уведомлению РКН о начале обработки ПДн (то самое «внестись в реестр операторов» или «стать оператором»). Часть 2 статьи 22 содержит условия, при которых возможно осуществлять обработку ПДн без уведомления, однако по собственному опыту, рекомендую в любом случае уведомить РКН, от этого не будет хуже. Также в статье 22 описан порядок подачи и рассмотрения уведомления со стороны РКН. Уведомление представляет из себя стандартизированную форму на сайте РКН <https://pd.rkn.gov.ru/operators-registry/notification/form/>. Полагаю, возможно осуществлять «тестовое» заполнение без ограничений, форма содержит те вопросы, ответы на которые мы получаем на стадии анкетирования (перечень ИСПДн, принятые технические и организационные меры, сведения об оборудовании, сведения об используемых СЗИ, перечень обрабатываемых ПДн, категории субъектов, категории данных). При необходимости, можно изучить форму Уведомления посредством тестового заполнения и скорректировать вопросы в анкете (для аудита) с учётом сведений, запрашиваемых в Уведомлении.

20. **Статья 22.1 №152-ФЗ** содержит обязательное требование о назначении лица, ответственного за организацию обработки ПДн в компании. Лицо назначается Приказом руководителя или иного уполномоченного лица, у Лица должна быть инструкция или дополнение к должностной инструкции. Ответственное лицо осуществляет взаимодействие с субъектами при наличии запросов с их стороны, соблюдение требований к процессам обработки, ознакомление сотрудников с необходимыми документами (первичный инструктаж).

21. **Статьи 23 и 23.1** описывают права и обязанности РКН, а также порядок осуществления государственного контроля. Следует отметить, что Постановление Правительства РФ от 29.06.2021 N 1046 регламентирует порядок проведения проверки со стороны РКН, также существует Приказ Роскомнадзора от 24.12.2021 N 253, содержащий «проверочный лист», используемый при проверках РКН, по данному листу наиболее

предпочтительно сверяться выполненную работу, скриншот пункта листа для примера:

11.	Обрабатываются ли контролируемым лицом специальные категории персональных данных в случаях, предусмотренных частями 2 и 2.1 статьи 10 Закона о персональных данных?	часть 2 статьи 10 Закона о персональных данных		
-----	---	--	--	--

22. **Статья 24** ссылается на законодательство, регулирующее ответственность в сфере нарушений обработки ПДн(скриншот ниже):

☐ "Трудовой кодекс Российской Федерации" от 30.12.2001 N 197-ФЗ (ред. от 06.04.2024) Статья 81. Расторжение трудового договора по инициативе работодателя в) разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника; Статья 90. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника Статья 192. Дисциплинарные взыскания
☐ "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 22.04.2024, с изм. от 24.05.2024) Статья 5.39. Отказ в предоставлении информации Статья 13.11. Нарушение законодательства Российской Федерации в области персональных данных Статья 13.12. Нарушение правил защиты информации Статья 13.13. Незаконная деятельность в области защиты информации Статья 13.14. Разглашение информации с ограниченным доступом Статья 19.7. Непредставление сведений (информации)
☐ "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 06.04.2024) Статья 137. Нарушение неприкосновенности частной жизни Статья 140. Отказ в предоставлении гражданину информации Статья 272. Неправомерный доступ к компьютерной информации

23. **Статья 25** – заключительные положения.

24. В рамках промежуточного подведения итогов, следует обратить внимание на следующее:

- в рамках аудита процессов обработки проверить наличие и содержание согласий субъектов на обработку, выявить избыточные данные и исключить их из процесса сбора, установить правовые основания обработки;
- определить способы обработки ПДн (**статья 3 №152-ФЗ**), категории субъектов, перечень обрабатываемых данных, категории персональных данных;
- выявить необходимость использования письменной формы согласия, при использовании письменной формы согласия по требованиям закона, проверить соответствие письменной формы требованиям **статьи 9 №152-ФЗ**;
- установить наличие или отсутствие процессов передачи ПДн третьим лицам, основания такой передачи и наличие согласия субъектов на передачу (или наличие необходимого пункта о передаче в Согласии), также определить актуальность вопросов трансграничной передачи;
- уделить особое внимание Специальной и Биометрической категории ПДн (**статьи 10 и 11 №152-ФЗ**), при наличии возможности постараться исключить обработку указанных категорий;
- разработать и утвердить формы документов, необходимых для взаимодействия с субъектом ПДн в рамках соблюдения прав субъекта и обязанностей Оператора, предусмотренных №152-ФЗ;
- выполнить требования, предусмотренные **главой 4 №152-ФЗ (статьи 18 – 22.1)**, в том числе организационные и технические меры, указанные непосредственно в статьях, а также требования **ПП №1119** и **Приказа ФСТЭК №21**;

- собрать сведения, необходимые для подачи уведомления в РКН, о включении в реестр Операторов ПДн. При наличии организации в реестре, проверить актуальность размещенных в реестре сведений, внести соответствующие изменения (требования о внесении изменений в уведомление содержатся в **части 7 статьи 22**)

25. Отдельно подчеркну информацию относительно проверок, план проверок РКН находится в открытом доступе на официальных сайтах территориального органа РКН <https://78.rkn.gov.ru/p4657/p14117/> (Северо-Западный). Ссылки на документы, определяющие порядок проведения проверок и проверочный лист есть по тексту выше.

26. Уточнение в части определения перечня ИСПДн, согласно №152-ФЗ недопустимо объединять базы данных, обработка которых осуществляется в целях, несовместимых между собой. Данным принципом следует руководствоваться при определении перечня ИСПДн, например, ИСПДн «файловый сервер» и ИСПДн «Электронная почта» не следует объединять в единую ИСПДн, так как используются разные меры защиты, хранятся разные категории данных, используются различные способы и цели обработки. Но и чрезмерно «раздувать» количество ИСПДн не стоит, так как согласно требованиям **ПП №1119 (14 пункт Постановления)**, в рамках применения мер 3-его уровня защищенности необходимо назначить лицо, ответственное за безопасность ИСПДн (администратор безопасности). Возможно, назначить одно лицо, однако не во всех случаях возможно найти сотрудника, согласного нести ответственность за все системы сразу.

27. Также при разграничении ИСПДн следует руководствоваться физическим размещением структурных подразделений и вычислительной техники. Кроме того, следует учитывать физическое размещение при ограничении доступа (списки доступа), и не забывать про порядок допуска обслуживающего (технического) персонала в помещения, в которых обрабатываются ПДн или находится оборудование, являющиеся частью ИСПДн.

**Краткий обзор Постановления Правительства №1119 (ПП №1119)
«Об утверждении требований к защите персональных
данных при их обработке в информационных системах персональных
данных»**

28. Наиболее простым и понятным отображением ПП №1119 будет являться таблица, подобная этой, которую можно найти в интернете по запросу «таблица ПП №1119», однако актуальность таблицы следует проверять и производить сверку результатов с актуальной (действующей)

Категории ПДн		Специальные			Биомет- рические	Иные			Общедоступные		
Собственные работники		нет	нет	да		нет	нет	да	нет	нет	да
Количество субъектов		более 100 тыс.	менее 100 тыс.			более 100 тыс.	менее 100 тыс.		более 100 тыс.	менее 100 тыс.	
Тип актуальных угроз	1	1 УЗ	1 УЗ	1 УЗ	1 УЗ	1 УЗ	1 УЗ	1 УЗ	2 УЗ	2 УЗ	2 УЗ
	2	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	3 УЗ	3 УЗ	2 УЗ	3 УЗ	3 УЗ
	3	2 УЗ	3 УЗ	3 УЗ	3 УЗ	3 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ

29. Как уже было указано ранее, определив параметры, содержащиеся в таблице, мы можем установить для ИСПДн требуемый уровень защищенности, все параметры ясны, за исключением Типа актуальных угроз. Типы актуальных угроз указаны в пункте 6 ПП №1119, существует 3 типа:

- **Угрозы 1-го типа** актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе;

- **Угрозы 2-го типа** актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе;

- **Угрозы 3-го типа** актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Если максимально упростить, как правило, в типовой коммерческой организации, не обрабатывающей какие-либо особые категории данных, при использовании лицензионного программного обеспечения будет 3-ий тип актуальных угроз. Третий тип наиболее «популярен» при категорировании ИСПДн, так как позволяет среднестатистической коммерческой ИСПДн присвоить 4 или 3 уровень защищенности (в таблице пометка «УЗ»), которые значительно отличаются по составу базовых технических требований, указанных в Приказах ФСТЭК (в частности №21).

30. Все параметры категорирования ИСПДн по уровню защищенности указаны в **пунктах 8-12** Постановления №1119.

31. Пункты 13-16 устанавливают обязательные требования к ИСПДн, в зависимости от определенного уровня защищенности, для обеспечения 4-

ого уровня защищенности необходимо (буквенные обозначения буквально из ПП №1119):

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

32. Требования каждого последующего уровня «поглощают» перечень требований предыдущего (4ый уровень был описан в пункте выше, является пунктом 13 в Постановлении. Пункт 14 предусматривает выполнение требований пункта 13 (4ый уровень), а также назначение администратора безопасности ИСПДн:

13. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

14. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных [пунктом 13](#) настоящего документа, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

33. Требования 2-ого УЗ предполагают разграничение доступа к логам, а 1-ый УЗ предполагает наличие структурного подразделения ИБ или возложение функций ИБ на действующее структурное подразделение, а также (как я полагаю), наличие срабатываний на изменение полномочий сотрудников, с доступом к ПДн (SIEM, SoC, и аналогичное):

☆ 15. Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных [пунктом 14](#) настоящего документа, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

16. Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных [пунктом 15](#) настоящего документа, необходимо выполнение следующих требований:

а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

34. Соответственно не стоит забывать о принципе «поглощения» предыдущего уровня, если необходимо выполнять требования 2-ого УЗ, то учитывать следует пункты 13, 14, 15 Постановления №1119, а при выполнении требований 4-ого УЗ – только пункт 13, для 1-ого УЗ – все перечисленные требования и требования пункта 16 Постановления №1119.

35. Последний (17ый) пункт Постановления №1119 указывает, что контроль примененных требований можно осуществлять самостоятельно (периодический аудит соблюдения требований) или с привлечением юридических лиц и ИП, имеющих соответствующую лицензию на требуемый вид деятельности (лицензии ФСТЭК и ФСБ (в случае работы с СКЗИ или гостайной), также существуют лицензии Минобороны, но мы их не рассматриваем.

36. В рамках промежуточного вывода следует обобщить, что работа с требованиями ПП №1119 может выполняться после получения исходных данных (анкетирование, аудит процессов), уровень защищенности определяется в отношении каждой отдельной ИСПДн. Не следует привязывать определение Типа актуальных угроз к разработке модели угроз, Тип актуальных угроз, как и уровень защищенности возможно «оформить» одним актом, с перечнем ИСПДн, вводных данных для определения УЗ и итогом (заключением) комиссии по определению УЗ (Комиссия назначается Приказом, состоит из числа сотрудников Оператора, желательно иметь типовую форму положения и Приказа об утверждении комиссии, а также Акта и протокола собрания комиссии.

37. Задача ПП №1119 – произвести категорирование ИСПДн на основании вводных данных, и перейти к определению перечня технических мер, указанных в **Приказе ФСТЭК №21**.

38. Приказ ФСТЭК №21 содержит сведения о различных требованиях, в том числе к классу вычислительной техники и средств защиты информации. Для наилучшего восприятия документа, рекомендую условно «разбить» его

на 2 части, текстовая часть и Приложение (таблица). В соответствии с определенным УЗ ИСПДн (на предыдущем этапе) обращаемся сначала к приложению и определяем набор мер, отмеченный знаком «+» в столбце с нужным уровнем защищенности. После определения мер, обращаемся к текстовой части и читаем необходимые пояснения по применению данных мер.

39. Обширные методические указания по выполнению мер Приказа ФСТЭК №21 мне не встречались, но у ФСТЭК есть такие указания для выполнения мер ФСТЭК №17 <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-11-fevralya-2014-g>. Из предлагаемого документа можно многое уточнить, относительно мер Приказа ФСТЭК №21, так как они имеют схожие требования и ФСТЭК №17 с точки зрения логики – строже, так как регламентирует обработку в ГИС.

40. В завершение рассмотрел бы несколько кратких вопросов, которые обычно спрашивают:

А как и когда будут проверять?

Проверять будут если попадешь в план проверок, или в случае внеплановой проверки, для которой должны быть основания. Проверка бывает выездной и документарной, более точно это можно узнать в документе, регламентирующем проведение проверок.

А что проверяют?

На практике, по-разному происходит, но с точки зрения теории – все ограничено и предусмотрено проверочным листом и порядком проведения проверок

Как стать Оператором ПДн?

Все, кто обрабатывает ПДн – являются Операторами, даже физ.лица. Уведомление в РКН подается для внесения в открытый реестр Операторов, во исполнение требований №152-ФЗ

Какие требования выполнять?

№152-ФЗ, ПП №1119, Приказы ФСТЭК, Приказы ФСБ, Руководящие документы уполномоченных ФОИВ и ЦБ РФ. Профильные требования (ФОИВ и ЦБ) обычно известны сотрудникам, либо размещены на официальных сайтах ведомств или специальных порталах, а также посредством рассылки по подведомственным организациям

Как выполнять требования?

При отсутствии необходимости выполнения отдельных требований или отсутствия технической возможности, требуется задокументировать такой факт и принять соответствующие компенсационные меры ИБ. Не запрещено пользоваться методическими документами по выполнению требований в других сферах (например ГОСТ 57580), требования во многих случаях аналогичные, однако некоторые документы содержат больше контекстной информации.

Какие документы разработать?

Перечень необходимых документов для коммерческой организации нигде не определен, есть обязательные документы, которые прямо указаны (например: Политика обработки ПДн, Приказ о назначении ответственного лица, инструкции такого лица (лиц) и т.д. Итоговый перечень Оператор определяет самостоятельно, даже при изучении информации из открытых источников, возможно найти несколько десятков различных шаблонов, форм согласий, журналов и т.д. Возможно даже сделать один документ, на мой взгляд, главное чтобы по своему содержанию он отвечал на вопросы, поставленные в проверочном листе РКН и в целом документировал те требования и меры, которые были выполнены в ходе построения системы защиты ПДн.

Сколько ИСПДн вот «нормально?» 10 нормально?

Нормально

Можно ли просто сделать одну большую ИСПДн?

Можно, если это не противоречит принципам №152-ФЗ, в части соотношения целей обработки ПДн

Так что по итогу нужно сделать?

Определить бизнес-процессы обработки ПДн, их перечень, соотнести процессы обработки и перечень ИСПДн, произвести категорирование и определить уровень защищенности (ПП №1119), уточнить перечень мер в соответствии с УЗ, согласно Приказу ФСТЭК №21. В случае использования СКЗИ для защиты ПДн – не забыть про Приказ №378 ФСБ России. Если еще и на бумаге обрабатывают, то ПП №687 (неавтоматизированная обработка).

Проверить меры, содержащиеся в статьях 18-22.1 №152-ФЗ, проверить избыточность/достаточность собираемых ПДн относительно заявленных целей обработки, а также проверить содержание согласий на обработку (и их наличие).

Не забыть про требования обработки ПДн сотрудников, регламентируемых ТК РФ (обычно кадры в курсе процессов, но лучше с ними проработать этот момент)

Подать или актуализировать уведомление

Проверить наличие подтверждения ознакомления сотрудников с необходимыми документами, провести ознакомление если оно не проводилось

Актуализировать Политику обработки ПДн, проверить наличие неограниченного доступа к ней

Провести техническую инвентаризацию ИТ-активов и СЗИ, поставить вопрос о замене устаревшего оборудования

СЗИ, не имеющие сертификата ФСТЭК России – провести этапы ввода в эксплуатацию, т.е. сделать какую-никакую оценку соответствия, как того требует №152-ФЗ, если использовать сертифицированные средства защиты информации нет возможности.

Обратиться к методическим рекомендациям (в том числе профильных ведомств, в них тоже может быть полезная информация) при отсутствии понимания выполнения требований.

С точки зрения документов, если вообще ничего не понятно, следует документировать процессы, которые проходят с точки зрения ИБ, например, сканирование сканером уязвимостей создает запрос на разработку регламента Управления уязвимостями, порядок выявления, периодичность, ответственных за процесс, журнал проведения сканирования, отчёт/акт о проведении сканирования и далее по аналогии.