МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

ОРГАНИЗАЦИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

ОБОРОТ И ЭКСПЛУАТАЦИЯ СРЕДСТВ ШИФРОВАНИЯ

Примерный План-график внедрения и контроля мероприятий по безопасной обработке персональных данных, обороту и эксплуатации СКЗИ

Примерный План-график внедрения и контроля мероприятий по техническому оснащению информационных систем обработки персональных данных, по обороту и эксплуатации СКЗИ при обработке персональных данных

1. Защита персональных данных в мировой практике

В 1990 году была принята резолюция ООН о защите персональных данных. Есть конвенция Совета Европы 1981 года, ее подписало большинство европейских государств, для них этот документ обязателен и должен приниматься во внимание при разработке внутреннего законодательства. Существует также директива Европейского Сообщества 1995 года, которая касается защиты данных.

2. Законодательство о персональных данных в РФ

В Российской Федерации с 1 июля 2011 года вступил в силу закон №152-ФЗ от 27 июля 2006 года «О персональных данных». В сферу действия данного закона попадают все юридические и физические лица, которые обрабатывают персональные физических лиц. Закон требует, в частности, чтобы каждая организация, владеющая персональными данными, обеспечила их конфиденциальность. В случае нарушения положений закона компания может лишиться лицензии, аккредитаций и подвергнуться судебному преследованию со стороны граждан, чьи приватные записи были скомпрометированы. За неисполнение закона возможна гражданская, уголовная, административная, дисциплинарная и иная предусмотренная законодательством РФ ответственность.

Персональные данные — это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Даже связка имени и адреса электронной почты уже относится к персональным данным.

Обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными

Обработка персональных данных может осуществляться с согласия субъекта персональных данных или на других законных основаниях.

Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей.

Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных Федеральным законом «О персональных данных».

В организациях обрабатываются, как минимум, персональные данные:

- работников;
- близких родственников работников;
- кандидатов на вакантную должность;
- прочих физических лиц (учеников, студентов, клиентов, постояльцев, пациентов и т.д.)

Защита персональных данных при неавтоматизированной и автоматизированной обработке персональных данных, в том числе создание системы защиты персональных данных является прямой обязанностью оператора и обусловлена требованиями Федерального Закона Российской Федерации «О персональных данных».

3. Уполномоченные контролирующие и надзорные органы

Правом проводить контрольно-надзорные мероприятия (проверки) на предмет соблюдения законодательства о персональных данных обладают три федеральных органа исполнительной власти (регуляторы):

- Федеральная служба по надзору в сфере связи, массовых коммуникаций и информационных технологий (Роскомнадзор);
- Федеральная служба по техническому и экспортному контролю (ФСТЭК России);
- Федеральная служба безопасности Российской Федерации (ФСБ России).

Каждый из регуляторов может проводить проверки операторов персональных данных в пределах своих полномочий.

Роскомнадзор, как главный регулятор в этом вопросе, осуществляет контроль и надзор за выполнением требований Федерального закона «О персональных данных», в ведении ФСТЭК России находятся вопросы технической защиты информации, применение средств криптографической защиты информации в информационных системах персональных данных находится под надзором ФСБ России. Причем ФСБ России и ФСТЭК России при осуществлении контроля и надзора не имеют права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

Плановая проверка не может проводиться чаще, чем один раз в три года.

4. Проверка Роскомнадзора

4.1. Общий порядок проверки на предмет соблюдения законодательства о персональных данных Роскомнадзором:

Плановые и внеплановые проверки проводятся должностными лицами Роскомнадзора в форме документарной или выездной проверки. Количественный состав участников проверки должен быть не менее двух должностных лиц.

Плановые проверки проходят в соответствии с ежегодными планами по организации и проведению государственного контроля (надзора) за соответствием деятельности операторов, осуществляющих обработку персональных данных, являющихся государственными органами, юридическими и физическими лицами, требованиям законодательства Российской Федерации в области персональных данных размещаются на официальном сайте Роскомнадзора и доступны для ознакомления.

Внеплановые проверки проводятся по следующим основаниям:

- истечение срока исполнения Оператором ранее выданного предписания об устранении выявленного нарушения установленных требований законодательства Российской Федерации в области персональных данных.
- поступление в Службу Роскомнадзора или ее территориальные органы обращений и заявлений граждан, юридических лиц, индивидуальных предпринимателей, информации от органов государственной власти, органов местного самоуправления, из средств массовой информации, в том числе о следующих фактах:

  а) возникновение угрозы причинения вреда жизни, здоровью граждан
  б) причинение вреда жизни, здоровью граждан

- приказ Роскомнадзора, изданный в соответствии с поручениями Президента Российской Федерации, Правительства Российской Федерации, и на основании требования прокурора о проведении внеплановой проверки в рамках надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям.

Непосредственно перед проверкой, в адрес проверяемой организации направляется уведомление с копией приказа «О проведении проверки». В приказе указываются:

- место проведения проверки и наименование организации, в отношении которой проводится проверка;
- основания для проведения проверки (плановая проверка или в связи с другим законным основанием);
- перечень уполномоченных лиц;
- перечень привлекаемых к проверке лиц (эксперты сторонних организаций и т.д.)
- сроки проведения проверки;
- цели и задачи проверки;
- предметы контроля проверки;
- перечень документов, предоставление которых юридическим лицом необходимо для достижения целей и задач проверки;
- перечень территориальных органов Роскомнадзора привлекаемых к проведению отдельных мероприятий контроля;
- другие сведения.

4.2. Примерный перечень документов, представление которых проверяемым лицом необходимо для достижения целей и задач проведения проверки:

- копия документа о назначении должностного лица или уполномоченного представителя, которое обязано представлять интересы юридического лица, индивидуального предпринимателя при проведении проверки;
- организационно – штатная структурная схема юридического лица (до структурного подразделения);
- журнал учета проверок юридического лица, индивидуального предпринимателя, проводимых органами государственного контроля (надзора), органами муниципального контроля;
- уведомление об обработке персональных данных;
- письмо о внесении изменений в уведомление об обработке персональных данных (в случае возникновения изменений должно быть отправлено не позднее 10 рабочих дней с даты их возникновения);
- документы, подтверждающие обработку заявленных оператором персональных данных: снимок экрана (скриншот) - в случае осуществления автоматизированной обработки персональных данных; локальные акты, устанавливающие перечень обрабатываемых оператором персональных данных;
- письменное согласие субъектов персональных данных (в том числе работников) на обработку их персональных данных, составленное в соответствии с требованиями ст. 9 Федерального закона № 152-ФЗ от 27.07.2006г. «Об обработке персональных данных»;
- документы (согласие субъектов персональных данных на обработку их данных, нормативные правовые акты), подтверждающие наличие полномочий у оператора на обработку специальных категорий персональных данных (состояние здоровья, расовая и национальная принадлежность, политические взгляды, религиозные и философские убеждения, состояние интимной жизни) и биометрических персональных данных, а также документы (локальные акты оператора), подтверждающие соблюдение требований законодательства Российской Федерации при обработке указанных категорий персональных данных;
- локальные акты, регламентирующие порядок и условия обработки персональных данных, (положения, инструкции об автоматизированной и (или) неавтоматизированной обработке персональных данных работников оператора, иных субъектов персональных данных; листы ознакомления сотрудников, допущенных к обработке персональных данных без использования средств автоматизации, о факте обработке ими персональных данных и иных обстоятельствах, предусмотренных п.6 Постановления Правительства РФ № 687 от 15.09.2008г.);
- локальные акты, устанавливающие порядок уничтожения, а также подтверждающие уничтожение оператором персональных данных субъектов персональных данных по достижении цели обработки (например, акты об уничтожении материальных носителей персональных данных);
- описание помещений, в которых осуществляется обработка персональных данных: расположение, номера помещений; наличие охраны, режима обеспечения безопасности, оборудование помещений; общее количество рабочих мест, количество рабочих мест, на которых обрабатываются персональные данные; описание ЭВМ, носителей, на которых производится обработка персональных данных наименование, заводской, инвентарный номер (ЭВМ, носителей персональных данных); наличие средств шифрования (криптозащиты); средств имитозащиты (аппаратные, программные, аппаратно-программные средства, системы и комплексы) - наименование, заводской, инвентарный номер;
- локальные акты, определяющие список лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;
- локальные акты, устанавливающие лиц, ответственных за обработку перс. данных;

- договоры оператора с третьими лицами, в случае, если оператор на основании такого договора поручает им обработку персональных данных (договор обязательного медицинского страхования работающих граждан; договоры, о зачислении денежных средств на счета физических лиц (работников оператора) в соответствии с реестрами, предоставляемыми на электронных носителях; договоры с медицинским учреждением о прохождении обязательного медицинского осмотра работающих граждан);
- документы, подтверждающие выполнение оператором мер, предусмотренных статьями 18.1 и 19 Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных»; документы, подтверждающие выполнение оператором при обработке персональных данных необходимых организационных мер для защиты персональных данных от неправомерного или случайного доступа к ним;
- журналы (книги) учёта применяемых средств защиты информации, носителей персональных данных (ЭВМ, дискеты и т.п.); сертификат (ФСТЭК, ФСБ) о возможности эксплуатации средств защиты информации; приказ о составе комиссии по классификации информационных систем персональных данных; документальное оформление присвоения информационной системе соответствующего класса (Акт об определении уровня защищенности ПДн в ИСПДн); электронный журнал обращений пользователей информационной системы на получение персональных данных; журнал учета периодических проверок информационной системы соответствующими должностными лицами (работниками) оператора или уполномоченного лица; соответствующие документы организации охраны, режима обеспечения безопасности (приказы, другие документы);
- журнал обращений граждан, локальный нормативный акт, утверждающий форму и порядок ведения журнала обращений граждан;
- типовые формы документов, предполагающие или допускающие содержание персональных данных (заявления, анкеты и др.);
- локальные акты оператора, регламентирующие порядок хранения материальных носителей персональных данных;
- журнал (реестр, книга) для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор (при наличии).

Перечень представляемых документов может быть уточнён в ходе проверки.

Если на проверку отведены двадцать дней, это не означает, что сотрудники Роскомнадзора все выделенное время будут находиться в проверяемой организации. Скорее всего, будет запланировано несколько встреч. На первую встречу, как правило, сотрудники РКН привозят бумажную версию Уведомления о проведении плановой выездной проверки оператора, выполняют оценку и определяют масштаб мероприятий, назначают дату следующего встречи. Обычно с этого момента процесс считается официально запущенным.

Следующий визит чаще всего рассматривают как основной, где сотрудники Роскомнадзора, согласно уведомлению оператора, проверяют внесенные изменения и в случае необходимости оставляют свои комментарии. Дальше могут последовать вопросы к сотрудникам основных отделов. Когда речь касается обработки персональных данных, опрашиваются организации и компании, с которыми возникает обмен ПДн. Это могут быть кадровые агентства, банки, операторы связи и прочие организации.

Как показывает практика, в ходе проверки может быть запрошено гораздо большее количество документов по сравнению с тем, что требовалось изначально. По результатам проверки Роскомнадзор выдает акт с указанием выявленных нарушений, если таковые были обнаружены, справку о результатах плановой выездной проверки, а также предписание об устранении в установленный срок выявленных несоответствий.

Предписание Роскомнадзора должно быть выполнено точно в срок. В противном случае организацию ждет повторная проверка или возбуждение дела об административном правонарушении.

4.3. Типичные нарушения при проверке Роскомнадзора

Типичными нарушениями, выявленными при проверке организаций, являются следующие:

- отсутствие в организации распорядительных документов, регламентирующих порядок обработки персональных данных;
- обработка персональных данных осуществляется без соответствующего согласия субъекта персональных данных;
- предоставление организацией неполных или недостоверных сведений, содержащихся в уведомлении Роскомнадзора об обработке персональных данных;
- нарушение требований конфиденциальности, допущенное при обработке персональных данных;
- несоответствие содержания письменного согласия субъекта персональных данных перечню, установленному Федеральным законом «О персональных данных»;
- отсутствует соблюдение требований законодательства в области персональных данных при передаче персональных данных без соответствующего согласия субъекта персональных данных;
- отсутствие в агентских договорах условий обеспечения безопасности персональных данных при их обработке;
- отсутствуют перечень ИСПДн, модель угроз, проект по созданию защиты персональных данных, сертификаты на средства защиты информации;
- не проведена оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных (ИСПДн);
- отсутствует документ подтверждающий соответствие ИСПДн Оператора требованиям действующего законодательства по защите персональных данных (например, Аттестат).

За нарушение требований законодательства в области защиты персональных данных предусмотрена административная и уголовная ответственность.

5. Проверка ФСБ России

Плановые и внеплановые проверки проводятся должностным лицом или должностными лицами, уполномоченными на проведение проверки, которые указаны в распоряжении или приказе начальника уполномоченного подразделения ФСБ России либо лица его замещающего.

Плановые проверки проходят в соответствии с ежегодными планами по организации и проведению в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных Правительством РФ, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

План проверок ФСБ России на год публикуется на официальном сайте Генеральной прокуратуры РФ. Здесь любая организация по своему ИНН или ОГРН может узнать о предстоящих проверках в текущем году, их длительности и периоде проведения.

Регулярный контроль использования шифровальных средств, применяемых для обеспечения безопасности персональных данных (далее ПДн), проводится на основании требований следующих нормативно-методических документов ФСБ России:

- приказ ФСБ от 10 июля 2014 года №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»;
- приказ ФСБ России от 9 февраля 2005 года №66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13 июня 2001 года №152;
- «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденные руководством 8 Центра ФСБ России (№ 149/7/2/6-432 от 31.03.2015).

ФСБ России интересуют средства криптографической защиты. Здесь кроется масса нюансов: учет и хранение средств шифрования, допуски к СКЗИ, регламент их использования должны проводиться в строгом соответствии с требованиями законодательства.

Нарушение правил защиты информации, согласно статье 13.12 КоАП РФ, может повлечь ряд санкций: штрафы для должностных лиц и организации, а также конфискацию самих средств криптозащиты. Следствием может стать невозможность отправить электронную отчетность или блокировка работы организации в системе обмена данными.

Для того чтобы подготовиться к проверке ФСБ России, необходимо провести ряд организационных мер, разработать и утвердить документы, связанные с работой с СКЗИ.

Ответы на следующие вопросы помогут систематизировать работу по подготовке к проверке и сосредоточиться на необходимых мерах:

- Есть ли в организации средства криптографической защиты информации? Есть ли документы на их приобретение, ведется ли учет? Какими документами регламентируется передача СКЗИ в отчуждение и в пользование?
- Какое подразделение в организации отвечает за работу с СКЗИ, а именно: составление заключений о возможности эксплуатации СКЗИ, разработку мероприятий по обеспечению функционирования и безопасности применяемых СКЗИ в соответствии с условиями выданных на них сертификатов, поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним, учет обслуживаемых обладателей конфиденциальной информации, контроль за соблюдением условий использования СКЗИ, расследование и составление заключений по фактам нарушения условий использования СКЗИ, разработку схемы организации криптографической защиты конфиденциальной информации?
- Какими документами регламентируется создание обозначенного выше подразделения, а также какими документами назначаются лица, ответственные за выполнение действий в рамках данного подразделения?
- Выработан ли регламент учета и хранения СКЗИ?

- Утверждены ли формы журналов учета СКЗИ? Как они ведутся?
- Определен ли круг ответственных лиц и ответственность в случае нарушения правил работы с СКЗИ?
- Каким образом производится хранение и предоставление доступа к СЗКИ?
- Все документы должны быть утверждены руководителем либо уполномоченным лицом организации, грифов конфиденциальности (и не в коем случае секретности) не требуется, однако документы должны быть предназначены только для сотрудников организации и проверяющих.

5.1. Предметы контроля (организационные и технические меры) операторов персональных данных использующих СКЗИ для обеспечения безопасности персональных данных при их обработке в информационных системах

Для 4 уровня защищенности:

1. Решение оператора персональных данных (ПДн) об использовании СКЗИ для обеспечения безопасности ПДн при их обработке в информационных системах (модель угроз и модель нарушителя).
2. Соответствие выбранного класса СКЗИ в соответствии с таблицей:

Уровень защищенности ПДн	4 УЗ	3 УЗ		2 УЗ			1 УЗ	
Тип актуальных угроз	3	2	3	1	2	3	1	2
Минимальный класс СКЗИ	КС1	КВ	КС1	КА	КВ	КС1	КА	КВ

3. 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. (Действующий сертификат соответствия ФСБ России).
4. Формуляр на СКЗИ.
5. Установочный комплект (дистрибутив на CD).
6. Организационные и технические меры, определенные в эксплуатационных документах на СКЗИ (формуляр, инструкция по эксплуатации).
7. 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.
8. Обеспечение сохранности носителей персональных данных.
9. Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей.
10. Акт уничтожения ключевого документа.
11. Годовой отчет в ОКЗИ об уничтоженной ключевой информации.
12. Журнал поэкземплярного учета СКЗИ.
13. Технический (аппаратный) журнал.
14. Журнал учета опломбирования.
15. Журнала учета носителей персональных данных с использованием регистрационных (заводских) номеров.
16. Заключение о возможности эксплуатации СКЗИ.
17. Заключение о допуске пользователей СКЗИ.
18. План проведения проверок за соблюдением условий использования СКЗИ.
19. Утверждение руководителем оператора документа, определяющего Правила доступа в Помещения с СКЗИ в рабочее и нерабочее время, а также в нештатных ситуациях.

20. Схема организации криптографической защиты.
21. Приказ о допуске пользователей к работе с СКЗИ.
22. Приказ о назначении ответственного пользователя СКЗИ.
23. Утверждение руководителем оператора документа, определяющего функциональные обязанности ответственного пользователя СКЗИ.
24. Оснащение Помещений входными дверьми с замками, обеспечение постоянного закрытия дверей Помещений с СКЗИ на замок и их открытия только для санкционированного прохода, а также опечатывания Помещений с СКЗИ по окончании рабочего дня или оборудование Помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии Помещений с СКЗИ.

Для 3 уровня защищенности:

1. Все предметы контроля для 4 уровня защищенности.
2. Назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе, обладающего достаточными навыками обеспечения безопасности персональных данных в информационной системе.

Для 2 уровня защищенности:

1. Все предметы контроля для 4 и 3 уровня защищенности.
2. Выполнение требования о том, 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.

Для 1 уровня защищенности:

1. Все предметы контроля для 4, 3 и 2 уровня защищенности.
2. Создание отдельного структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение его функций на одно из существующих структурных подразделений.
3. Обеспечение информационной системы автоматизированными средствами, позволяющими автоматически регистрировать в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе.
4. Отражение в электронном журнале безопасности полномочий сотрудников оператора персональных данных по доступу к персональным данным, содержащимся в информационной системе. Указанные полномочия должны соответствовать должностным обязанностям сотрудников оператора.
5. Назначение оператором лица, ответственного за периодический контроль ведения электронного журнала безопасности и соответствия отраженных в нем полномочий сотрудников оператора их должностным обязанностям (не реже 1 раза в месяц).
6. Оборудовать окна Помещений с СКЗИ, расположенные на первых и (или) последних этажах зданий, а также окна Помещений, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в Помещения посторонних лиц, металлическими решетками или ставнями, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения.
7. Оборудовать окна и двери Помещений с СКЗИ, в которых размещены серверы информационной системы, металлическими решетками, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения.

5.2. Программа проведения работ по контролю (надзору) за использованием шифровальных (криптографических) средств, применяемых для обеспечения безопасности персональных данных в информационных системах персональных данных

№ п/п	Проверяемые требования	Перечень представляемых документов и справок
1	Организация системы организационных мер защиты персональных данных: - область применения средств криптографической защиты информации (далее - СКЗИ) в информационных системах персональных данных; - наличие ведомственных документов и приказов по организации криптографической защиты информации; - выполнение рекомендаций и указаний ФСБ России (при их наличии) по вопросам организации связи с использованием криптосредств.	Ведомственные документы и приказы по организации криптографической защиты информации.
2	Организация системы криптографических мер защиты информации: - наличие модели угроз нарушителя; - соответствие модели угроз исходным данным; - соответствие требуемого уровня криптографической защиты полученной модели нарушителя; соответствие используемых СКЗИ полученному уровню криптографической защиты; - наличие документов по поставке СКЗИ оператору.	Модель угроз, разработанная оператором. Документы по поставке СКЗИ оператору.
3	Разрешительная и эксплуатационная документация: - наличие необходимых лицензий для использования СКЗИ в информационных системах персональных данных; - наличие сертификатов соответствия на используемые СКЗИ; - наличие эксплуатационной документации на СКЗИ (формуляров, правил работы, руководств оператора и т.п.); - порядок учета СКЗИ, эксплуатационной и технической документации к ним; - выявление несертифицированных ФСБ России (ФАПСИ) СКЗИ.	Лицензии и сертификаты на используемые СКЗИ. Эксплуатационная документация на СКЗИ.
4	Требования к обслуживающему персоналу: - порядок учета лиц, допущенных к работе с СКЗИ, предназначенными для обеспечения безопасности персональных данных в информационной системе; - наличие функциональных обязанностей ответственных пользователей СКЗИ; - укомплектованность штатных должностей личным составом, а также достаточность имеющегося личного состава для решения задач по организации криптографической защиты информации;	Утвержденные список лиц, допущенных к работе с СКЗИ. Документы, подтверждающие функциональные обязанности сотрудников.

	- организация процесса обучения лиц, использующих СКЗИ, применяемых в информационных системах, правилам работы с ними и другим нормативным документам по организации работ (связи) с использованием СКЗИ.	Журнал учета пользователей криптосредств. Документы, подтверждающие прохождение обучения сотрудников.
5	Эксплуатация СКЗИ: - проверка правильности ввода СКЗИ в эксплуатацию и соответствие условий эксплуатации технических средств удостоверяющего центра (при наличии) требованиям эксплуатационной документации и сертификатов соответствия; - оценка технического состояния СКЗИ, соблюдения сроков и полноты проведения технического обслуживания, а также проверка соблюдения правил пользования СКЗИ и порядка обращения с ключевыми документами к ним.	Акты ввода СКЗИ в эксплуатацию. Журнал поэкземплярного учета СКЗИ. Журнал учета и выдачи носителей с ключевой информацией.
6	Оценка соответствия применяемых СКЗИ: - соответствие программного обеспечения, реализующего криптографические алгоритмы используемых СКЗИ, эталонным версиям, проходивших сертификацию в ФСБ России; - проведение (при необходимости) на местах осуществления проверки оперативных тематических исследований используемых СКЗИ.	Средства СКЗИ. Программное обеспечение СКЗИ (дистрибутив).
7	Организационные меры: - выполнения требований по размещению, специальному оборудованию, охране и организации режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним, а также соответствия режима хранения СКЗИ и ключевой документации предъявляемым требованиям; - оценка степени обеспечения оператора криптоключами и организации их доставки. - проверка наличия инструкции по восстановлению связи в случае компрометации действующих ключей к СКЗИ. - порядок проведения разбирательств и составления заключений по фактам нарушения условий хранения носителей персональных данных или использования СКЗИ.	Эксплуатационная документация на СКЗИ. Помещения, выделенные для установки СКЗИ и хранения ключевых документов к ним. Инструкция по восстановлению связи в случае компрометации действующих ключей к СКЗИ.

При проведении проверки должностные лица ФСБ России вправе допускаться к СКЗИ, техническим средствам, на которых они реализованы, оборудованию комплексов, в помещения, в которых установлены СКЗИ, к средствам технической защиты, предназначенным для хранения, обработки и передачи персональных, и ключевых документов.

По результатам проверки должностными лицами ФСБ России, проводящими проверку, составляется акт в двух экземплярах, один из которых с копиями приложений, вручается оператору,

осуществляющему обработку персональных данных, или уполномоченному им лицу под расписку об ознакомлении или отказе в ознакомлении с актом проверки.

В журнале учёта проверок должностными лицами ФСБ России осуществляется запись о проведённой проверке, содержащая сведения о датах начала и окончания проведения проверки, времени её проведения, правовых основаниях, целях, задачах и предмете проверки, выявленных нарушениях и выданных предписаниях, а также указываются фамилии, имена, отчества и должности должностного лица или должностных лиц, проводящих проверку, его или их подписи (При отсутствии журнала учёта проверок в акте проверки делается соответствующая запись).

5.3. Типичные нарушения при проверке ФСБ России

Нарушения и недостатки, выявленные в ходе проверок, можно разделить на 4 категории:

1. Нарушения, связанные с разработкой внутренних нормативных документов:

- не определен уровень защищенности ПДн в ИСПДн;
- отсутствуют или требуют доработки модели угроз или нарушителя;
- отсутствует инструкция о порядке действий при компрометации ключей.

2. Нарушения, связанные с порядком эксплуатации средств криптографической защиты информации (далее - СКЗИ):

- использование СКЗИ, не прошедших сертификацию ФСБ России;
- использование СКЗИ с истекшими сроками действия сертификатов;
- использование ключей с истекшими сроками их действия;
- отсутствие формуляров, эксплуатационной и технической документации;
- аппаратные средства, совместно с которыми эксплуатируется СКЗИ, не оборудованы средствами контроля за их вскрытием.

3. Нарушения, связанные с подготовкой и назначением пользователей криптосредств:

- не назначен ответственный пользователь;
- отсутствует список лиц, допущенных к работе с СКЗИ;
- лица, допущенные к работе с СКЗИ, не проходят обучение и не ознакомлены с действующими нормативными и методическими документами.

4. Нарушения, связанные с учетом и хранением СКЗИ и ключевой документации к ним:

- не ведется учет СКЗИ, ключевых документов, эксплуатационной и технической документации;
- хранилища и помещения с СКЗИ не оборудуются приспособлениями для опечатывания, либо личные печати отсутствуют;
- не пронумерованы и не учтены ключи от помещений с СКЗИ.

6. Риски

По итогам проверок, мер систематического наблюдения и жалоб физических лиц Роскомнадзор и другие проверяющие органы могут накладывать штрафы, аннулировать лицензии, дисквалифицировать должностных лиц и блокировать сайты.

Основные риски:

- наложение на организацию штрафа до 300 000 рублей;
- наложение на должностных лиц штрафа до 20 000 рублей;
- разрыв трудового договора с должностным лицом;
- запрет руководителю занимать руководящие должности на срок до 3-х лет;
- блокировка сайта организации по жалобе физического лица;
- внесение компании в реестр нарушителей прав субъектов персональных данных.

С 1 сентября 2015 года Роскомнадзор имеет право без проверки, на основании жалобы физического лица заблокировать сайт организации за несоблюдение требований закона «О персональных данных».

7. Ответственность (по состоянию на 01.07.2017г.)

Административная ответственность, предусмотренная за нарушение требований законодательства в области защиты персональных данных

Согласно ст. 24 Федерального закона "О персональных данных" от 27.07.2006 N 152-ФЗ, на лиц, виновных в нарушении его требований, возлагается гражданская, уголовная, административная, дисциплинарная и иная предусмотренная законодательством РФ ответственность. При этом способ реагирования на выявленное правонарушение определяет соответствующий контролирующий орган самостоятельно в пределах имеющихся у него полномочий.

Приводим ниже полный вариант статьи 3.11 КоАП РФ в новой редакции от 7 февраля 2017 года, вступившую в силу с 1 июля 2017 года.

«Статья 13.11. Нарушение законодательства Российской Федерации в области персональных данных

1. Обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи, если эти действия не содержат уголовно наказуемого деяния, -

влечет предупреждение или наложение административного штрафа на граждан в размере от **одной тысячи до трех тысяч рублей**; на должностных лиц - от **пяти тысяч до десяти тысяч рублей**; на юридических лиц - от **тридцати тысяч до пятидесяти тысяч рублей**.

2. Обработка персональных данных без согласия в письменной форме субъекта персональных данных на обработку его персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством Российской Федерации в области персональных данных, если эти действия не содержат уголовно наказуемого деяния, либо обработка персональных данных с нарушением установленных законодательством Российской Федерации в области персональных данных требований к составу сведений, включаемых в согласие в письменной форме субъекта персональных данных на обработку его персональных данных, -

влечет наложение административного штрафа на граждан в размере от **трех тысяч до пяти тысяч рублей**; на должностных лиц - от **десяти тысяч до двадцати тысяч рублей**; на юридических лиц - от **пятнадцати тысяч до семидесяти пяти тысяч рублей**.

3. Невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки персональных данных, или сведениям о реализуемых требованиях к защите персональных данных -

влечет предупреждение или наложение административного штрафа на граждан в размере от **семисот до одной тысячи пятисот рублей**; на должностных лиц - от **трех тысяч до шести тысяч рублей**; на индивидуальных предпринимателей - от **пяти тысяч до десяти тысяч рублей**; на юридических лиц - от **пятнадцати тысяч до тридцати тысяч рублей**.

4. Невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных, -

влечет предупреждение или наложение административного штрафа на граждан в размере от **одной тысячи до двух тысяч рублей**; на должностных лиц - от **четырех тысяч до шести тысяч рублей**; на индивидуальных предпринимателей - от **десяти тысяч до пятнадцати тысяч рублей**; на юридических лиц - от **двадцати тысяч до сорока тысяч рублей**.

5. Невыполнение оператором в сроки, установленные законодательством Российской Федерации в области персональных данных, требования субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, -

влечет предупреждение или наложение административного штрафа на граждан в размере от **одной тысячи до двух тысяч рублей**; на должностных лиц - от **четырех тысяч до десяти тысяч рублей**; на индивидуальных предпринимателей - от **десяти тысяч до двадцати тысяч рублей**; на юридических лиц - от **двадцати пяти тысяч до сорока пяти тысяч рублей**.

6. Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих в соответствии с законодательством Российской Федерации в области персональных данных сохранность персональных данных при хранении материальных носителей персональных данных и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении персональных данных, при отсутствии признаков уголовно наказуемого деяния -

влечет наложение административного штрафа на граждан в размере от **семисот до двух тысяч рублей**; на должностных лиц - от **четырех тысяч до десяти тысяч рублей**; на индивидуальных предпринимателей - от **десяти тысяч до двадцати тысяч рублей**; на юридических лиц - от **двадцати пяти тысяч до пятидесяти тысяч рублей**.

7. Невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обезличиванию персональных данных либо несоблюдение установленных требований или методов по обезличиванию персональных данных -

влечет предупреждение или наложение административного штрафа на должностных лиц в размере от **трех тысяч до шести тысяч рублей**.";

Защита конфиденциальных данных предусмотрена ст. 13.14 КоАП РФ. Если лицо, получившее доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, разгласило ее, то на него будет наложен административный штраф в размере от **4000 до 5000 рублей**.

Возможно применение и иных статей КоАП РФ к нарушителям закона о ПД.

Статья 5.39 КоАП РФ. Отказ в предоставлении гражданину информации. Неправомерный отказ в предоставлении гражданину информации об обработке его персональных данных. Штраф: для должностных лиц - от **1000 до 3000 рублей**.

Статья 13.12 КоАП РФ. Нарушение правил защиты информации. Штраф: для должностных лиц - от **1500 до 2500 рублей**; для юридических лиц - от **15000 до 20000 рублей**.

Статья 13.14 КоАП РФ. Разглашение информации с ограниченным доступом. Штраф: для граждан - от **500 до 1000 рублей**; а для должностных лиц - от **4000 до 5000 рублей**.

Также отвечать придется и за непредоставление информации в уполномоченный орган (Роскомнадзор). В этом случае в соответствии со статьей 19.7 КоАП грозит наложение штрафа на должностных лиц - от **300 до 500 рублей**; на юридических лиц - от **3000 до 5000 рублей**. Например, нарушением статьи 19.7. КоАП РФ является не предоставление в Уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) уведомления о своем намерении осуществлять обработку персональных данных субъектов. За невыполнение законного предписания Роскомнадзора (например, предписания об устранении выявленных нарушений) могут оштрафовать по статье 19.5 КоАП. При этом сумма штрафа составит для должностных лиц - от **1000 до 2000 рублей**; для юридических лиц - от **10000 до 20000 рублей**.

Уголовная ответственность

К уголовной ответственности нарушителей закона о ПД могут привлечь по двум статьям.

Статья 137 УК РФ Нарушение неприкосновенности частной жизни. Незаконное собирание или распространение персональных данных либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации. Штраф до **200000 рублей**, либо обязательные работы до **360 часов**, либо исправительные работы до **1 года**, либо принудительными работами на срок до **двух лет**, либо арест до **4 месяцев**, либо лишением свободы на срок до **двух лет**.

Статья 272 УК РФ Неправомерный доступ к компьютерной информации. В этом случае грозит штраф до **200000 рублей** или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительные работы на срок **до одного года**, либо лишение свободы на срок до **двух лет**.

8. Защита персональных данных при их обработке в организации

Разделим все требования для простоты на 4 группы. Работая с персональными данными, вы должны:

1. Подготовить и принять пакет организационно-распорядительной документации.
2. Привести процессы работы с персональными данными в соответствие с законом.
3. Реализовать техническую защиту персональных данных в информационных системах и провести Оценку эффективности принимаемых мер по обеспечению безопасности персональных данных.
4. Хранить базы с персональными данными на территории Российской Федерации.

8.1. Требования по подготовке внутренних организационно-распорядительных документов

Статья 18.1 Федерального закона «О персональных данных» требует от операторов персональных данных иметь локальные акты и политику, регламентирующую обработку и защиту персональных данных. Точного перечня необходимых документов не предполагается и жестких требований о количестве подлежащих разработке локальных актов оператора действующим законодательством не установлено.

Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законодательством Российской Федерации в области персональных данных. Это меры организационного, правового и технического характера.

Практика реализации этих мер сформировала необходимый минимум документов, который должен быть принят оператором, это:

- общий документ, определяющий политику оператора в отношении обработки персональных данных;
- локальный акт или несколько актов, которые могут включать в себя описание всех процессов обработки персональных данных, включая перечень лиц, имеющих доступ к персональным данным, порядок обеспечения доступа и работы с персональными данными, процесс уничтожения персональных данных. Указанные акты также должны содержать конкретное описание правовых, организационных и технических мер 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;
- локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

8.2. Требования по приведению процессов работы с персональными данными в соответствие с законом

Персональные данные необходимо правильно собирать, обрабатывать и передавать.

Со всеми физическими лицами, у которых вы собираете персональные данные (например, через сайт клиента), должен быть заключен договор или взято согласие на их обработку.

С каждым контрагентом, которому вы передаете, предоставляете в доступ (например, другому оператору на субподряд) или от которого получаете персональные данные, необходимо заключить соглашение о поручении на их обработку.

Все сотрудники должны под роспись ознакомиться с внутренними документами организации по обработке и защите персональных данных и подписать обязательство о неразглашении.

В Роскомнадзор должно быть подано уведомление об обработке персональных данных.

8.3. Требования по технической защите персональных данных в информационных системах (для технических специалистов организации)

Если персональные данные хранятся или как-то иначе обрабатываются в информационных системах (например, в «1С: Бухгалтерии», в базе данных сайта и других), нужно определить уровень их защищенности, составив соответствующий акт, опираясь на Таблицу 1.

Таблица 1. Определение уровня защищенности ПДн в ИСПДн.

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1 тип (НДВ в СПО)	2 тип (НДВ в ППО)	3 тип (нет НДВ)
Специальные	Не сотрудников	Более 100 000	УЗ 1	УЗ 1	УЗ 2
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Любое	УЗ 1	УЗ 2	УЗ 3
Биометрические	Любых	Любое	УЗ 1	УЗ 2	УЗ 3
Иные	Не сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 3	УЗ 4
	Сотрудников	Любое	УЗ 1	УЗ 3	УЗ 4
Общедоступные	Не сотрудников	Более 100 000	УЗ 2	УЗ 2	УЗ 4
		Менее чем 100 000	УЗ 2	УЗ 3	УЗ 4
	Сотрудников	Любое	УЗ 2	УЗ 3	УЗ 4

От уровня защищенности персональных данных в ИСПДн зависит объем мероприятий по их защите, выбор сертифицированных средств защиты информации и СКЗИ в соответствии с Таблицей 2, Таблицей 3 и Таблицей 4 соответственно.

Таблица 2. Определение минимального перечня мероприятий по ЗИ.

Перечень мер защиты	1 УЗ	2 УЗ	3 УЗ	4 УЗ
Организовать режим обеспечения безопасности помещений, в которых размещена ИСПДн, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих прав доступа в эти помещения	+	+	+	+
Обеспечить сохранность носителей ПДн	+	+	+	+
Утвердить перечень лиц, имеющих доступ к ПДн в рамках выполнения своих служебных обязанностей	+	+	+	+
Использовать сертифицированные СЗИ	+	+	+	+
Назначить приказом должностное лицо, ответственное за обеспечение безопасности ПДн в ИСПДн.	+	+	+	
Доступ к электронному журналу сообщении определить только лицам, которым необходимы сведения, содержащиеся в данном журнале для выполнения своих служебных обязанностей	+	+		
Обеспечить автоматическую регистрацию в электронном журнале безопасности изменения полномочии сотрудника по доступу к ПДн в ИСПДн	+			

Перечень мер защиты	1 УЗ	2 УЗ	3 УЗ	4 УЗ
Создать структурное подразделение ответственное за обеспечение безопасности ПДн в ИСПДн или возложить эти функции по обеспечению безопасности ПДн в ИСПДн на одно из существующих структурных подразделении	+			

Таблица 3. Определение минимального класса защиты СЗИ.

	УЗ1		**УЗ2**		**УЗ3**			**УЗ4**
	АУ1, АУ2 или АУ3 с ССОП	**АУ3 без подключения к ССОП**	**АУ1, АУ2 или АУ3 с ССОП**	**АУ3 без подключения к ССОП**	**АУ2**	**АУ3 с подключения к ССОП**	**АУ3 без подключения к ССОП**	**-**
СВТ	5 класс СВТ		5 класс СВТ		5 класс СВ			6 класс СВТ
СОВ	4 класс СОВ и 4 НДВ		4 класс СОВ и 4 НДВ		4 класс СОВ и 4 НДВ	4 класс СОВ	5 класс СОВ	5 класс СОВ
САЗ	4 класс САЗ и 4 НДВ		4 класс САЗ и 4 НДВ		4 класс САЗ и 4 НДВ	4 класс САЗ	5 класс САЗ	5 класс САЗ
МЭ	3 класс МЭ и 4 НДВ	4 класс МЭ и 4 НДВ	3 класс МЭ и 4 НДВ	4 класс МЭ и 4 НДВ	3 класс МЭ и 4 НДВ	3 класс МЭ	4 класс МЭ	5 класс МЭ
Другие СЗИ	Любое ТУ или 3Б и 4 НДВ		Любое ТУ или 3Б и 4 НДВ		Любое ТУ или 3Б и 4 НДВ	Любое ТУ или 3Б		Любое ТУ или 3Б
УЗ - уровень защищенности ИСПДн **СВТ** - средство вычислительной техники			**АУ** -максимальный тип актуальных угроз **СОВ** - средство обнаружения вторжении **САЗ** - средство антивирусной защиты			**ССОП** - сеть связи общего пользования (Интернет) **МЭ** - межсетевое экранирование		

Таблица 4. Определение минимального класса СКЗИ.

Уровень защищенности ПДн	4 УЗ	3 УЗ		2 УЗ			1 УЗ	
Тип актуальных угроз	3	2	3	1	2	3	1	2
Минимальный класс СКЗИ	КС1	КВ	КС1	КА	КВ	КС1	КА	КВ

Затем нужно разработать модель угроз (документ, назначение которого выявить и обосновать возможные угрозы обрабатываемым Вами персональным данным, методы несанкционированного доступа к персональным данным, злоумышленников, которые могут быть заинтересованы в компрометации обрабатываемых Вами персональных данных) и на основании Постановления Правительства № 1119 и Приказа ФСТЭК России № 21 составить техническое задание на создание системы защиты персональных данных.

После этого разрабатывается и внедряется проект системы защиты с применением конкретных видов средств защиты информации и обеспечением необходимых организационных мероприятий.

Внедрением может заняться сама организация или подрядчик, имеющий соответствующую лицензию ФСТЭК России, ФСБ России.

Отдельно отмечаем, что лицензируются не только услуги (т.е. работы, выполняемые для третьих лиц), но и отдельные виды работ (т.е. те работы, которые выполняются в т.ч. и для себя), поэтому будьте внимательны, чтобы не нарушить соответствующие требования к наличию лицензионных разрешений.

8.4. Требования по хранению баз персональных данных на территории Российской Федерации

С 1 сентября 2015 года сбор и хранение персональных данных граждан Российской Федерации может происходить только на территории Российской Федерации.

О месторасположении баз данных необходимо уведомить Роскомнадзор.

Особенно это касается иностранных и российских компаний, чьи информационные системы полностью или частично располагаются за пределами РФ.

Проверку локализации баз персональных данных Роскомнадзор проводит просто — запрашивает договор с российским хостинг-провайдером.

Примерный План-график внедрения и контроля мероприятий по безопасной обработке персональных данных, обороту и эксплуатации СКЗИ при их обработке

№п/п	Вид ОРД	Когда утверждается/ кем утверждается	Когда контролируется/ актуализируется	Ответственный за контроль/дата очередного контроля	Отметка об исполнении/ дата
Организационно-распорядительное обеспечение					
1	Приказ об утверждении комиссии по определению уровня защищенности	При организации работ по защите ПДн /руководителем организации	При изменении состава комиссии / в начале года (рекомендовано, но не обязательно)	ФИО	**Исполнено**
1.1	от «___» _____ №_____	руководитель (ФИО)_____	члены комиссии: (ФИО)	«___»_____	
2	Приказ об обеспечении безопасности персональных данных	При организации работ по защите ПДн /руководителем организации	В соответствии с утвержденным планом мероприятий. В начале года (рекомендовано, но не обязательно). В обычном режиме - не реже 1 раза в 2 года/ При изменении условий обработки ПДн, расширении ИСПДн, добавлении новых ИСПДн.	ФИО	**Исполнено**
2.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
3	Приказ об определении границ контролируемой зоны	При организации работ по защите ПДн /руководителем организации	В соответствии с утвержденным планом. Контролируется не реже 1 раза в 2 года/ При изменении границ контролируемой зоны.	ФИО	**Исполнено**
3.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____ _____	

№п/п	Вид ОРД	Когда утверждается/ кем утверждается	Когда контролируется/ актуализируется	Ответственный за контроль/дата очередного контроля	Отметка об исполнении/ дата
4	Приказ об утверждении перечня информационных систем ПДн.	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		**Исполнено**
4.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
5	Приказ об утверждении мест хранения материальных носителей ПДн.	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
5.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
6	Приказ об утверждении перечня должностей.	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
6.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
7	Приказ об утверждении перечня ПДн	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
7.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
8	Приказ об утверждении политики в области обработки ПДн	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
8.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	

№п/п	Вид ОРД	Когда утверждается/ кем утверждается	Когда контролируется/ актуализируется	Ответственный за контроль/дата очередного контроля	Отметка об исполнении/ дата
9	Приказ об утверждении положения об ответственном за организацию защиты ПДн	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
9.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
10	Приказ об утверждении положения по обработке ПДн	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
10.1	от «___» _____ №_____	Руководитель (ФИО)_____ _		«___»_____	
11	Приказ об утверждении правил внутреннего контроля	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
11.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
12	Приказ об утверждении порядка оценки вреда субъектам ПДн	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
12.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
13	Приказ об утверждении правил работы с обезличенными ПДн	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
13.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
14	Приказ об утверждении правил рассмотрения запросов субъектов ПДн	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не		

№п/п	Вид ОРД	Когда утверждается/ кем утверждается	Когда контролируется/ актуализируется	Ответственный за контроль/дата очередного контроля	Отметка об исполнении/ дата
			реже 1 раза в 2 года		
14.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
15	Приказ об уничтожении ПДн	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
15.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
16	Приказ об утверждении типовых форм	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
16.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
17	Приказ о порядке доступа в помещения	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
17.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
18	Приказ о назначении лица представляющего организацию	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
18.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
19	Приказ об утверждении правил неавтоматизированной обработки ПДн	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		

№п/п	Вид ОРД	Когда утверждается/ кем утверждается	Когда контролируется/ актуализируется	Ответственный за контроль/дата очередного контроля	Отметка об исполнении/ дата
19.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
20	Приказ об утверждении положения по работе с инцидентами информационной безопасности	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
20.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
21	Приказ о журнале учета посетителей	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
21.1	от «___» _____ №_____	Руководитель (ФИО)_____ _		«___»_____	
22	Журнал проведения инструктажа	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
22.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
23	Журнал резервного копирования	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
23.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
24	Журнал учета инцидентов	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
24.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	

№п/п	Вид ОРД	Когда утверждается/ кем утверждается	Когда контролируется/ актуализируется	Ответственный за контроль/дата очередного контроля	Отметка об исполнении/ дата
25	Журнал учета машинных носителей	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
25.1	от «___» _____ №_____	Руководитель (ФИО)_____ _		«___»_____	
26	Журнал учета обращений субъектов ПДн	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
26.1	от «___» _____ №_____ _	Руководитель (ФИО)_____ _		«___»_____	
27	Журнал учета проверок юридических лиц	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
27.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
28	Журнал регистрации передачи ПДн	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
28.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
29	Акт оценки вреда субъектам ПДн	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
29.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
30	Инструкция о порядке проведения разбирательств	При организации работ по защите ПДн	В соответствии с утвержденным планом		

№п/п	Вид ОРД	Когда утверждается/ кем утверждается	Когда контролируется/ актуализируется	Ответственный за контроль/дата очередного контроля	Отметка об исполнении/ дата
		/ руководителем организации	мероприятий/не реже 1 раза в 2 года		
30.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
31	Инструкция о порядке резервирования и восстановления	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
31.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
32	Инструкция по антивирусной защите	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
32.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
33	Инструкция по парольной защите	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
33.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
34	Инструкция по учету носителей ПДн	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
34.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
35	Инструкция для работников, допущенных к обработке ПДн	При организации работ по защите ПДн / руководителем организации При организации работ по защите ПДн /	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		

№п/п	Вид ОРД	Когда утверждается/ кем утверждается	Когда контролируется/ актуализируется	Ответственный за контроль/дата очередного контроля	Отметка об исполнении/ дата
		руководителем организации			
35.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
36	Инструкция ответственного лица за организацию обработки ПДн	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
36.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
37	План мероприятий по защите ПДн	При организации работ по защите ПДн / руководителем организации	На очередном отчетном собрании у руководителя/не реже 1 раза в год		
37.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
38	План проведения внутреннего контроля по ПДн	При организации работ по защите ПДн / руководителем организации	На очередном отчетном собрании у руководителя/не реже 1 раза в год		
38.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
39	Регламент информационного взаимодействия со сторонними ИС	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
39.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
40	Уведомление в Роскомнадзор	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
40.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	

№п/п	Вид ОРД	Когда утверждается/ кем утверждается	Когда контролируется/ актуализируется	Ответственный за контроль/дата очередного контроля	Отметка об исполнении/ дата
41	Наличие в договорах с контрагентами, предусматривающих обработку ПДн (в т.ч. передачу, хранение и т.д.), условий о выполнении мероприятий по охране ПДн		В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
41.1				«___»_____	
	Документальное обеспечение эксплуатационно-технического сопровождения средств криптографической защиты информации (СКЗИ)				
1	Приказ о назначении ответственного пользователя СКЗИ	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
1.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
2	Приказ о допуске пользователей к работе с СКЗИ	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
2.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
3	Функциональные обязанности ответственного пользователя СКЗИ	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
3.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
4	Инструкция по допуску лиц в помещения, где	При организации работ по защите ПДн	В соответствии с утвержденным		

№п/п	Вид ОРД	Когда утверждается/ кем утверждается	Когда контролируется/ актуализируется	Ответственный за контроль/дата очередного контроля	Отметка об исполнении/ дата
	ведется эксплуатация СКЗИ	/ руководителем организации	планом мероприятий/не реже 1 раза в 2 года		
4.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
5	Инструкция по работе с ключевыми носителями	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
5.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
6	Журнал технический (аппаратный) по СКЗИ	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
6.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
7	Журнал опломбирования аппаратных средств с СКЗИ	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
7.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
8	Журнал поэкземплярного учета ключевых документов	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
8.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
9	Акт уничтожения ключевого документа	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не		

№п/п	Вид ОРД	Когда утверждается/ кем утверждается	Когда контролируется/ актуализируется	Ответственный за контроль/дата очередного контроля	Отметка об исполнении/ дата
			реже 1 раза в 2 года		
9.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
10	Годовой отчет в орган криптографической защиты информации об уничтоженной ключевой информации	При организации работ по защите ПДн / руководителем организации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в год		
10.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
11	Заключение о возможности эксплуатации СКЗИ	При вводе в эксплуатацию/Орган криптографической защиты информации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
11.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
12	Заключение о допуске пользователей СКЗИ	При вводе в эксплуатацию/Орган криптографической защиты информации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
12.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
13	Схема организации криптографической защиты	При вводе в эксплуатацию/Орган криптографической защиты информации	В соответствии с утвержденным планом мероприятий/не реже 1 раза в 2 года		
13.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
14	План проведения проверок в области криптографии	При организации работ СКЗИ/ руководителем организации	На очередном отчетном собрании у руководителя/не реже 1 раза в год		
14.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	

№п/п	Вид ОРД	Когда утверждается/ кем утверждается	Когда контролируется/ актуализируется	Ответственный за контроль/дата очередного контроля	Отметка об исполнении/ дата
	Проектная и эксплуатационно-техническая документация на сервера и автоматизированные рабочие места				
1	Техно-рабочий проект системы защиты персональных данных	До ввода в эксплуатацию/Руководителем проектной организации и руководителем организации-собственника системы	1 раз в год /не реже 1 раза в 3 года		
1.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
2	Технический паспорт на ИСПДн	До ввода в эксплуатацию/ руководителем организации-собственника системы	1 раз в год /не реже 1 раза в 3 года		
2.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
3	Модель угроз ПДн в ИСПДн по методике ФСТЭК России	До ввода в эксплуатацию/Руководителем организации-разработчика и руководителем организации-собственника системы	1 раз в год /не реже 1 раза в 3 года		
3.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
4	Модель нарушителя безопасности ПДн по методике ФСБ России	До ввода в эксплуатацию/Руководителем организации-разработчика и руководителем организации-	1 раз в год /не реже 1 раза в 3 года		

№п/п	Вид ОРД	Когда утверждается/ кем утверждается	Когда контролируется/ актуализируется	Ответственный за контроль/дата очередного контроля	Отметка об исполнении/ дата
		собственника системы			
4.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
5	Перечень программных средств	До ввода в эксплуатацию/ Руководителем организации-собственника системы	1 раз в год /не реже 1 раза в 3 года		
5.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
6	Перечень информационных ресурсов	До ввода в эксплуатацию/ Руководителем организации-собственника системы	1 раз в год /не реже 1 раза в 3 года		
6.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
7	Матрица доступа к информационным ресурсам	До ввода в эксплуатацию/ Руководителем организации-собственника системы	1 раз в год /не реже 1 раза в 3 года		
7.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
8	Акт классификации автоматизированной системы	До ввода в эксплуатацию/ Руководителем организации-собственника системы	1 раз в год /не реже 1 раза в 3 года		
8.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
9	Акт по определению уровня защищенности ПДн в информационной системе ПДн	До ввода в эксплуатацию/ Руководителем организации-собственника системы	1 раз в год /не реже 1 раза в 3 года		

№п/п	Вид ОРД	Когда утверждается/ кем утверждается	Когда контролируется/ актуализируется	Ответственный за контроль/дата очередного контроля	Отметка об исполнении/ дата
9.1	от «___» _____ №_____	Руководитель (ФИО)__		«___»_____	
10	Описание технологического процесса	До ввода в эксплуатацию/ Руководителем организации-собственника системы	1 раз в год /не реже 1 раза в 3 года		
10.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	
11	Приказ о вводе в промышленную эксплуатацию	До ввода в эксплуатацию/ Руководителем организации-собственника системы	1 раз в год /не реже 1 раза в 3 года		
11.1	от «___» _____ №_____	Руководитель (ФИО)_____		«___»_____	

Примерный План-график внедрения и контроля мероприятий по техническому оснащению информационных систем обработки персональных данных, по обороту и эксплуатации СКЗИ при обработке персональных данных

№п/п	Вид обеспечения	Предмет контроля	Когда контролируется	Ответственный за контроль/дата очередного контроля	Отметка об исполнении/ дата
Техническое оснащение мероприятий по защите персональных данных					
1	Средства защиты информации: СЗИ НСД; САЗ; СКН; МЭ; СОВ.	Параметры конфигурации; Срок действия сертификата соответствия	В соответствии с утвержденным планом мероприятий, не реже 1 раза в год	ФИО	**Исполнено**
1.1	Акт установки от «___» _____ №_____			«___»_____	

№п/п	Вид обеспечения	Предмет контроля	Когда контролируется	Ответственный за контроль/дата очередного контроля	Отметка об исполнении/ дата
2	Автоматизированное рабочее место	Параметры конфигурации BIOS	В соответствии с утвержденным планом мероприятий, не реже 1 раза в год	ФИО	**Исполнено**
2.1				«___»_____	
3			В соответствии с утвержденным планом мероприятий, не реже 1 раза в год	ФИО	**Исполнено**
3.1				«___»_____	
4			В соответствии с утвержденным планом мероприятий, не реже 1 раза в год	ФИО	**Исполнено**
4.1					
Техническое оснащение мероприятий по обороту и эксплуатации СКЗИ при обработке персональных данных					
1	Охранная сигнализация, охранное видеонаблюдение (металлические решетки на окнах крайних этажей, окнах рядом с пожарными лестницами) мест размещения и эксплуатации СКЗИ	Наличие, работоспособность	В соответствии с утвержденным планом мероприятий, не реже 1 раза в год	ФИО	**Исполнено**
1.1				«___»_____	
2	Металлические шкафы, сейфы, места хранения СКЗИ	Наличие, наличие и работоспособность устройств опечатывания	В соответствии с утвержденным планом мероприятий, не реже 1 раза в год	ФИО	**Исполнено**
2.1				«___»_____	
3			В соответствии с утвержденным планом мероприятий, не реже 1 раза в год	ФИО	**Исполнено**

№п/п	Вид обеспечения	Предмет контроля	Когда контролируется	Ответственный за контроль/дата очередного контроля	Отметка об исполнении/ дата
3.1				«___»_____	
4			В соответствии с утвержденным планом мероприятий, не реже 1 раза в год	ФИО	**Исполнено**
4.1				«___»_____	