МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

М.И. Шубинский

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЛЯ РАБОТНИКОВ БЮДЖЕТНОЙ СФЕРЫ. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Учебное пособие

Санкт-Петербург

2013

Шубинский М. И. **Информационная безопасность для работников бюджетной сферы. Защита персональных данных: учебное пособие.** – СПб: НИУ ИТМО, 2013. –77 с.

Издание адресовано студентам магистерской программы «Управление государственными информационными системами» и слушателям дополнительной образовательной программы повышения квалификации «Электронное правительство и инновационные технологии управления», реализуемой Центром технологий электронного правительства НИУ ИТМО.

Рекомендовано к печати учёным советом Магистерского корпоративного факультета.

В 2009 г. университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена Программа развития государственного образовательного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет информационных технологий, механики и оптики» на 2009–2018 г.г.

Оглавление

Введение

Скачкообразное насыщение компьютерами государственных учреждений и органов власти и управления, произошедшее в начале 2000 годов в России породило целый ряд насущных проблем, связанных с внедрением информационных технологий в процесс управления. В результате последние 10 лет основной задачей стало выстраивание информационной среды учреждений. Эта чрезвычайно нужная и важная проблема отодвинула все более частные проблемы на второй план. Сейчас, когда уже можно говорить, что задача построения информационной среды успешно решена, начинают всплывать важнейшие проблемы, оставленные ранее до лучших времен.

Один из самых важных вопросов, стоящих сейчас перед любым государственным учреждением с точки зрения информационных технологий, — это вопрос информационной безопасности. Одним из ключевых направлений информационной безопасности является проблема обеспечения защиты персональных данных.

Целью данной работы является определить потенциальные объемы работ по защите персональных данных, стоящие перед государственным учреждением.

Учебное пособие «Информационная безопасность для работников бюджетной сферы. Защита персональных данных» предназначено для применения в рамках магистерской программы «Управление государственными информационными системами».

Курс (учебный модуль) предназначен также для использования в системе дистанционного обучения Магистерского корпоративного факультета НИУ ИТМО и ориентирован на реализацию дополнительной образовательной программы повышения квалификации «Электронное правительство и инновационные технологии управления». Программа реализуется Центром технологий электронного правительства НИУ ИТМО и ориентирована на повышение квалификации государственных и муниципальных служащих по вопросам развития электронного правительства, информационного общества, применения инновационных технологий управления, построения единого информационного пространства органов государственной власти и местного самоуправления, а также оптимизации управления на основе перевода государственных и муниципальных услуг в электронный вид.

Глава 1.
Что такое «персональные данные»?

Вопрос о защите личных (персональных) данных впервые на серьезном уровне был поднят в 1976 г., когда комитет министров Совета Европы принял решение о разработке конвенции «О защите физических лиц при обработке персональных данных, осуществляемой на международном уровне». Она была разработана в 1981 г. («О защите физических лиц при автоматизированной обработке персональных данных» ETS № 108, Страсбург, 28.01.1981) и открыта для подписания странами Европы. Конвенция защищает неприкосновенность частной жизни от избыточного и недобросовестного вмешательства в связи с обработкой персональных данных.

Конвенция ратифицирована в России (№ 160-ФЗ от 19.12.2005), после чего началось формирование нормативно-законодательной базы в сфере использования и защиты персональных данных. В 2006 г. Государственной думой РФ был принят базовый закон — федеральный закон № 152-ФЗ «О персональных данных», который чётко регламентировал все вопросы, касающиеся получения, использования, передачи и других действий с персональными данными, а также вопросы их защиты. Необходимо отметить, что государство, присоединяющееся к конвенции, вправе заявить о ее распространении также на данные, которые не проходят автоматической обработки, что было сделано в Российской Федерации.

Согласно базовому закону персональными данными является абсолютно любая информация, которая относится к определённому или определяемому (прямо или косвенно) физическому лицу. Основными персональными данными, которые встречаются в повседневной жизни, являются фамилия, имя, отчество субъекта (физического лица), дата рождения, адрес местожительства или регистрации, социальное, имущественное, семейное положение, сведения о доходах, образовании, профессии и т.п.

Существуют четыре категории персональных данных (ПДн), которые разделяются по степени информативности.

Первая категория включает в себя информацию о национальной и расовой принадлежности субъекта, о религиозных либо философских убеждениях, о здоровье и интимной жизни субъекта.

Вторая категория содержит информацию, по которой можно идентифицировать человека и получить дополнительные сведения, например, ФИО, адрес и сведения о заработках.

Третья категория — информация, позволяющая только определить субъекта, т.е., например, фамилия, имя и дата рождения.

К **четвертой категории** относятся общедоступные или обезличенные персональные данные. Общедоступными являются ПДн, которые в

соответствии с законодательством не могут подвергаться сокрытию, т.е. не могут быть конфиденциальными (например, сведения о доходах представителей органов государственной и муниципальной власти), либо ПДн, доступ к которым предоставлен с разрешения самого субъекта.

Обезличенными персональными данными является информация, по которой невозможно определить ее принадлежность конкретному физическому лицу.

Персональные данные с точки зрения британского закона о защите данных

Необходимо отметить, что, несмотря на вышеизложенные нормы, до сих пор неочевиден ответ на вопрос "Что такое персональные данные?"

Четкого алгоритма в российских нормативных документах пока нет, но есть очень интересный алгоритм в документах, принятых в Великобритании, который рассмотрим ниже [1]. Великобритания имеет гораздо больший, чем РФ, опыт по разработке нормативных документов в области персональных данных.

В британском законе о защите данных (Data Protection Act 1998, далее — DPA) к «персональным данным» относят информацию, которая

- представляет собой «данные», которые обрабатываются в компьютерных системах, либо без использования средств автоматизации в системах регистрации документов;
- относится к идентифицируемому на основании этих данных субъекту (физическому лицу).

Для того чтобы определить, являются ли конкретные данные «персональными» (согласно DPA), можно использовать алгоритм, заключающийся в ответах на 8 последовательных вопросов (как в службе поддержки продуктов Microsoft).

1. Идентифицируемость субъекта

Может ли живой индивидуум быть идентифицирован на основании этих данных или этих данных и другой информации, находящейся во владении оператора ПДн, или которая может с достаточной вероятностью оказаться у оператора ПДн?

Ответ «Да» — переходим к следующему вопросу.

Ответ «Нет» — эти данные не являются "персональными".

В большинстве случаев ФИО и некоторой дополнительной информации достаточно, чтобы идентифицировать субъекта. ФИО — это общепринятое средство идентификации людей на бытовом уровне, но одних ФИО недостаточно (по этому, в частности, придуманы паспорта), т.к. существуют полные тезки, то возможность идентифицировать кого-то по ФИО зависит от наличия дополнительной информации.

Например, «Иван Петрович» — это однозначно не персональные данные, т.к. таких в России много и непонятно о ком конкретно идет речь, а вот Иван Петрович, работающий в ГУ «Хозснаб», позволяет идентифицировать Ивана Петровича, если только в «Хозснаб» нет двух (или больше) Иванов Петровичей. В последнем случае для идентификации потребуется дополнительная информация (например, номер рабочего телефона), но и этого будет недостаточно, если два Ивана Петровича работают в одном отделе и имеют один и тот же служебный номер телефона. Тогда для идентификации конкретного Ивана Петровича потребуется еще информация о нем и т.д.

Сделаем вывод, что один и тот же набор данных в зависимости от контекста и конкретных обстоятельств может относиться как к «персональным» данным, так и не к таковым.

Конечно, если вам неизвестны имя и фамилия человека, то это не означает, что вы не можете его идентифицировать. Например, многие сослуживцы Ивана Петровича могут не знать его полного имени, однако это не мешает им его идентифицировать. Они могли бы его описать, например, следующим образом: "молодой человек, с темными волосами, работающий на втором этаже и приезжающий на работу на мотоцикле". Это абстрактное описание, как ни странно, позволяет идентифицировать Ивана Петровича, опять же если на втором этаже не работают несколько молодых людей, являющихся брюнетами и приезжающих на работу на мотоцикле.

Сделаем следующий вывод: для идентификации субъекта необязательно наличие его ФИО, паспортные данные и т.п., так как человека можно идентифицировать по косвенным признакам.

Таким образом, возможность идентифицировать субъекта по определенным данным, а, значит, и возможность квалифицировать данные как «персональные» (за исключением вполне очевидных или общепринятых ситуаций) зависит от различных факторов и определяется фактически на основании субъективных экспертных оценок и сложившейся практики. Например, с точки зрения европейской практики ФИО в сочетании с номером телефона, местом работы или домашним адресом в большинстве случаев вполне достаточно для идентификации субъекта.

Как видим, вопрос идентифицируемости субъекта является достаточно сложным и неоднозначным даже в европейском законодательстве о персональных данных, которому уже больше 20 лет, что тут говорить о нашем ФЗ-152, которому не исполнилось еще и 6 лет и в котором понятие персональных данных, хотя и позаимствовано из европейского, но не совпадает с ним.

Так, согласно ФЗ-152 «персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой

информации физическому лицу (субъекту персональных данных), *в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация»*.

Согласно UK Data Protection Act: «personal data» means data which relate to a living individual who can be identified — a) from those data, or b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, *and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual."*

Курсивом выделена та часть определений, которая существенно различается по смыслу. Из нашего определения исчезла та существенная часть, в которой говориться, что ПД — это данные, которые, в том числе, "включают в себя любое выражение мнения об индивидууме и любые признаки намерения оператора данных или любого другого лица в отношении индивидуума".

2. Относятся ли данные к идентифицируемому субъекту?

Относятся ли данные к идентифицируемому субъекту, к его личной или семейной жизни, трудовой или профессиональной деятельности?

Ответ «Да» — данные являются «персональными».

Ответ «Нет» — данные не принадлежат к числу «персональных».

Ответ «Может быть» — переходим к следующему вопросу.

Может показаться, что определить, относятся ли конкретные данные к человеку или нет, достаточно просто. Однако понятие «относится к» в законодательстве совсем не так очевидно. Вот что говорится об этом в британском техническом руководстве: *«Данные, позволяющие идентифицировать индивидуума даже без использования его имени, могут являться персональными в случае, если они обрабатываются с целью узнать или записать что-либо об этом индивидууме, или если обработка этих данных может повлиять на данного индивидуума»*.

Таким образом, данные могут «относиться к» субъекту несколькими различными способами.

3. Данные с очевидностью содержат информацию о субъекте

Очевидно ли, что данные содержат информацию о конкретном субъекте?

Ответ «Да» — это «персональные данные». Это — самый простой случай, когда данные, очевидно, представляют собой информацию о конкретном человеке, например, история болезни, уголовное дело, личное дело и т.п. Это следует из содержания этих данных.

Ответ «Нет» — переходим к следующему вопросу.

Действительно, данные могут содержать информацию не о конкретном человеке, а о действиях, совершаемых данным человеком, или о результатах этих действий.

В случаях, когда не представляется очевидным, что данные содержат информацию о конкретном человеке, следующие вопросы помогают определить, являются ли эти данные персональными:

Обрабатываются ли (или могли бы обрабатываться) эти данные с целью

- узнать что-либо;
- записать что-либо;
- принять какое-либо решение в отношении идентифицируемого индивидуума?

Можете ли вы узнать или записать что-либо об идентифицируемом индивидууме в результате случайных последствий обработки этих данных?

Может ли обработка этих данных оказать какое-либо воздействие или причинить ущерб идентифицируемому индивидууму?

Чтобы в этом разобраться, необходимо ответить на вопросы 4 — 8.

4. Данные, связанные с субъектом

Связаны ли данные с субъектом таким образом, что из них можно получить конкретную информацию об этом субъекте?

Ответ «Да» — это персональные данные.

Ответ «Нет» — переходим к следующему вопросу.

Во многих случаях данные сами по себе не являются персональными, но в определенных ситуациях они могут превращаться в персональные в том случае, если их можно связать с конкретным субъектом для того, чтобы получить о нем дополнительную информацию.

Например, данные о зарплате на должности ведущего специалиста «Хозснаб» сами по себе не являются персональными данными. Они могут указываться, например, в описании конкретных вакансий, и в этом случае они не являются персональными данными. Однако, когда те же данные о зарплате связаны с именем Ивана Петровича, они становятся персональными данными, связанными с конкретным работником, занимающим данную должность.

5. Цель обработки

Используются ли данные для принятия решения, затрагивающего интересы конкретного субъекта?

Ответ «Да» — это персональные данные.

Ответ «Нет» — переходим к следующему вопросу.

5.1. Информация, оказывающая влияние на принятие решений в отношении субъекта

Существует много примеров, когда данные относят к субъекту на основании того, что эти данные оказывают влияние на принятие решений в отношении субъекта. Например, данные о состоянии счета Ивана Петровича за телефонные переговоры позволяют определить, сколько он должен заплатить за эти услуги.

В таких случаях важны цели обработки данных. Данные о мотоцикле Ивана Петровича сами по себе не являются персональными, т.к. они о мотоцикле, а не о человеке. Однако в некоторых ситуациях эта информация может быть привязана к владельцу мотоцикла и рассматриваться как персональные данные Ивана Петровича. Например, объем двигателя мотоцикла с точки зрения налоговой службы влияет на размер транспортного налога, который платит Иван Петрович.

5.2. Обработка одних и тех же данных различными организациями в различных целях

Важно помнить о том, что один и тот же набор данных может являться персональными данными в одних руках и не являться ими в других. Например, на корпоративном празднике организации «Хозснаб» фотограф сделал фотографию участников и сохранил в электронной форме на компьютере. Изначально фотография не рассматривается в качестве персональных данных, поскольку она не используется для получения какой-либо информации о конкретном человеке. Однако возможен вариант, что на празднике случилась кража, и при расследовании следователь запросил эту фотографию, а затем использовал ее в качестве доказательства по уголовному делу. В этом случае данные, которые находясь у журналиста не относились к персональным, попав в руки следователя становятся персональными.

Сделаем вывод, что один и тот же набор данных, находясь у одного оператора, использующего его для одних целей, может не являться персональными данными, но, перейдя к другому оператору, использующему этот набор данных для других целей (при этом связывающего его с конкретным человеком), может становиться персональными данными и, соответственно, попадать под действие DPA.

6. Биографическое значение

Имеют ли данные какое-либо биографическое значение в отношении субъекта?

Ответ «Да» — данные (скорее всего) являются персональными.

Ответ «Нет» — переходим к следующему вопросу.

Ответ «Может быть» — переходим к следующему вопросу.

«Биографическое значение» данных надо рассматривать только в том случае, если неочевидно, что данные содержат сведения о субъекте или связаны с ним.

Информация может иметь биографическое значение для субъекта, если она содержит сведения о его местонахождении или деятельности в определенный период времени. Например, если Иван Петрович указан в качестве участника конференции, то отчет о данной конференции имеет биографическое значение для него, т.к. содержит сведения о его местонахождении в определенное время. Данный факт будет рассматриваться как персональные данные. Однако это не означает, что все содержимое отчета о конференции является персональными данными его участников. Возможно, в отчете о конференции будут и другие персональные данные об участниках, кроме их присутствия на конференции (ученая степень и т.п.), но это зависит от того, что является важным для составителя отчета.

7. Фокусировка информации на субъекте

Сфокусированы ли данные на субъекте как основном предмете или они, скорее, сфокусированы на ком-то другом: на объекте, процессе или событии?

Ответ «Да» — это (скорее всего) персональные данные.

Ответ «Нет» — переходим к следующему вопросу.

Ответ «Может быть» — переходим к следующему вопросу.

7.1. Отчет о конференции

Если на конференции рассматривалась квалификация конкретного Ивана Петровича, то запись данной дискуссии является его персональными данными. Однако это не означает, что весь отчет о конференции является персональными данными Ивана Петровича, т.к. на конференции наверняка обсуждали вопросы, никак к нему не относящиеся.

7.2. Информация не о субъектах, а об объектах

При рассмотрении вопроса о том, на чем сфокусирована информация, принимается во внимание цель обработки данной информации: записать сведения о субъекте или о каком-либо объекте. Например, может производиться запись информации о работе компьютерной программы. Если информация записывается с целью оценки качества программы, то она не относится к персональным данным. Однако, если информация записывается с целью оценки качества работы разработчика программы и от этого зависит размер премии, то информация о работе программы будет являться персональными данными программиста, разработавшего программу.

Более того, информация может являться персональными данными, даже если она только потенциально может быть использована для

получения каких-либо сведений о субъекте, как в приводимом далее примере.

8. Обработка информации, оказывающая влияние на субъекта

Могут ли данные оказать воздействие на человека в его личной, семейной, трудовой или профессиональной деятельности?

Ответ «Да» — это персональные данные.

Ответ «Нет» — эти данные навряд ли можно отнести к персональным.

8.1. Могут данные об объекте являться персональными данными субъекта, даже если оператор ПДн не использует в настоящее время эти данные для того, чтобы узнать, записать или принять какое-либо решение относительно субъекта?

Даже если данные не используются оператором персональных данных для получения информации о субъекте, в том случае, если имеются основания полагать, что эти данные могут быть использованы подобным образом, то они являются персональными.

Например, транспортная компания может отслеживать местоположение и маршруты перемещения своих транспортных средств в логистических целях. Эти данные используются для определения не местоположения конкретных водителей, а только для определения местонахождения ближайшего к месту загрузки транспортного средства. Однако в компании знают, какой водитель каким транспортным средством в настоящее время управляет, и потенциально могут использовать эту информацию для установления местонахождения конкретного водителя. Поэтому данные о местонахождении транспортных средств могут являться персональными данными водителей этих транспортных средств.

В результате можно сформулировать основную мысль.

Если данные позволяют (имеется реальная возможность) идентифицировать субъекта, и их обработка может причинить какой-либо ущерб его интересам (даже если цель их обработки в этом не состоит), то эти данные, скорее всего, являются персональными, если не доказано иное.

Контрольные вопросы

1. Как определяются персональные данные в 152 ФЗ?
2. Какие существуют четыре категории ПДн?
3. Какие данные называются «обезличенными»?
4. В чем разница в определении персональных данных 152 ФЗ и британского Data Protection Act?

Глава 2.
Законодательство по вопросам безопасности персональных данных

Законодательный уровень является важнейшим для обеспечения безопасности персональных данных. РФ. Ниже (рис.1) представлена примерная схема нормативных актов РФ, относящихся к вопросам безопасности персональных данных.

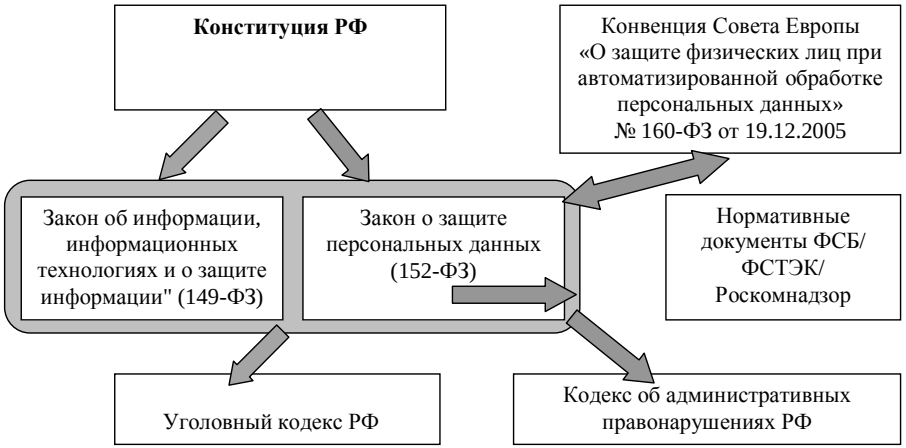

Рис. 1. Схема взаимодействия законодательных актов, имеющих отношение к защите персональных данных

Конституция РФ

Основным законом Российской Федерации, *затрагивающим вопросы информационной безопасности*, является Конституция, принятая 12 декабря 1993 г.

В соответствии **со статьей 23** гражданам должно обеспечиваться право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

В соответствии **со статьей 24** должно обеспечиваться право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

Статья 29 гарантирует свободу мысли и слова. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

Статья 41 гарантирует права на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей.

Статья 42 гарантирует права на знание достоверной информации о состоянии окружающей среды.

Наконец, **статья 55**, одна из важнейших, имеющих отношение к теме безопасности персональных данных, — права и свободы человека и гражданина могут быть ограничены федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Прежде чем переходить к нормативным документам Российской Федерации, посвященным защите персональных данных, необходимо отметить зарубежный документ, ставший отправной точкой в их разработке – это Конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» ETS № 108, Страсбург, 28.01.1981.

Россия присоединилась к конвенции лишь в середине первого десятилетия 21 века, ратифицировав ее Федеральным законом № 160-ФЗ от 19.12.2005.

Основная задача конвенции: обязать государства, подписавшие конвенцию, создать на национальном уровне полномасштабные законодательные регуляторы в сфере получения, обработки и защиты данных.

Основной мыслью концепции является то, что основу защиты прав личности составляют гарантии накопления и использования персональных данных только для точно определенных и законных целей, гарантии надлежащей защиты данных и доступности для индивидуума информации о себе, а эффективность государственной защиты персональных данных напрямую зависит от наличия независимого специализированного государственного органа, контролирующего государственных и негосударственных операторов.

Еще одной важной особенностью концепции было то, что государство, присоединяющееся к конвенции, вправе заявить о ее распространении также на данные, которые не проходят автоматической обработки.

В Российской Федерации был выбран именно такой вариант действий.

Закон «О персональных данных» №152-ФЗ от 2006 г.

Целью закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну (статья 2).

В законе в статье 3 дается определение **персональных данных**, которое мы уже рассматривали в 1-й главе.

В статье 5 говорится о принципах обработки персональных данных:

- законность целей и способов обработки персональных данных и добросовестность;
- соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;
- соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверность персональных данных, их достаточность для целей обработки, недопустимость обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимость объединения созданных для не совместимых между собой целей баз данных информационных систем персональных данных.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Статья 6 посвящена условиям обработки персональных данных. В частности обозначено, что обработка персональных данных может осуществляться оператором с согласия субъектов персональных данных. Согласия субъекта персональных данных не требуется в следующих случаях:

- обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;
- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

– обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

– обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

– осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

В статье 8 говорится об общедоступных источниках персональных данных.

В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

Статьей 10 регламентируется, что обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается. Исключение составляют угрозы здоровью субъекту персональных данных, обработка персональных данных в медико-профилактических и в правоохранительных целях и др. при соблюдении определенных условий.

В статье 14 описываются права субъекта персональных данных на доступ к своим персональным данным (на основании 24 статьи Конституции РФ).

В статье 19 говорится о мерах по обеспечению безопасности персональных данных при их обработке. В частности, что оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать

шифровальные (криптографические) средства для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

В статье 22 говорится об уведомлении об обработке персональных данных, что оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных.

Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных

– относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения;

– полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

– относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

– являющихся общедоступными персональными данными;

– включающих в себя только фамилии, имена и отчества субъектов персональных данных;

– необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

– включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

– обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

Закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. №149-ФЗ

Данный закон регулирует отношения возникающие при

– осуществлении права на поиск, получение, передачу, производство и распространение информации;

– применении информационных технологий;

– обеспечении защиты информации.

В **статье 3** закона говорится о принципах правового регулирования отношений, возникающих в сфере информации, информационных технологий и защиты информации:

– свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

– установление ограничений доступа к информации только федеральными законами;

– обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

– достоверность информации и своевременность ее предоставления;

– неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия.

В **статье 16** определяется понятие защиты информации.

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на

– обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

– соблюдение конфиденциальности информации ограниченного доступа;

– реализацию права на доступ к информации.

Иные нормативные документы

Кроме вышеуказанных законов, существует еще ряд нормативных документов, регламентирующих деятельность в области защиты персональных данных:

– Постановление Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

– Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации. Утверждено постановлением Правительства РФ № 687 от 15/09/2008.

– Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных».

– Приказ ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».Если рассмотреть вышеуказанные документы, то в соответствии с постановлением правительства №1119 и отменой действовавшего до конца октября 2012г. постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» требования по защите персональных данных в ИСПДн зависят от уровня защищенности ИСПДн.

Пока еще действующий 58-й приказ ФСТЭК во многом ужесточает нормы 152 ФЗ по защите персональных данных, что мы более подробно обсудим в заключительной главе, а так называемый «тройственный» приказ №55/86/20 рассмотрим в 3 главе настоящего пособия, когда будем говорить о классификации ИСПДн.

Контрольные вопросы

1. Какой закон РФ говорит о том, что люди имеют право знать о фактах, создающих угрозу для их жизни и здоровья?
2. Какая основная задача конвенции Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных»?
3. Какой закон регулирует отношения, возникающие при обеспечении защиты информации?
4. В каком случае сведения о субъекте персональных данных могут быть исключены из общедоступных источников персональных данных?

Глава 3.
Кто является оператором персональных данных? Классификация информационных систем персональных данных

Для того чтобы понять, кто же является оператором персональных данных, рассмотрим где же эти данные применяются (рис.2). Видно, что область применения персональных данных очень велика. Так ли это? Рассмотрим несколько примеров из разных областей деятельности.

Рис. 2. Области использования персональных данных

Проще всего дело обстоит с экономикой. На любом предприятии существует бухгалтерия, которая начисляет сотрудникам заработную плату. Можно с уверенностью сказать, что данные, хранящиеся в бухгалтерских программах, являются персональными, так как, кроме ФИО, содержат еще и паспортные данные, ИНН, номер страхового пенсионного свидетельства, сумму начисленной заработной платы и т.п. Персональными данными также являются реестр акционеров, кадрово-учетные дела и т.д. Особо надо отметить наличие у организаций персональных данных клиентов компании, например, вкладчиков банка или абонентов сотовой сети и т.п.

Если мы говорим о политике, то персональные данные есть в реестре избирателей и, например, в списках членов той или партии, причем эти данные являются данными самой высокой (1) категории (см. 1 главу), поскольку содержат информацию о политических предпочтениях. В

общественной и культурной сферах деятельности персональные данные содержатся в списках общественных объединений или участников тех или иных конкурсов и фестивалей. В социальной сфере специфические персональные данные есть и в образовании, и в медицине, и в работе с социальнонезащищенными гражданами. Так, в образовании это — и списки учащихся, и входящий в моду электронный дневник, и база получателей льготного (бесплатного) питания и т.п. В медицине это — данные пациентов, начинающиеся с данных страхового полиса обязательного медицинского страхования и адреса и заканчивающиеся диагнозами заболеваний (тоже 1 категория персональных данных), в социальной сфере это — прежде всего, реестр получателей государственной помощи, в котором также имеются данные 1 категории. Хочу обратить внимание, что мы обсуждаем только данные специфические для данной сферы деятельности. Поскольку экономические вопросы присущи абсолютно любым организациям, то список сотрудников будет и у бухгалтерии коммерческого банка, и у бухгалтерии театра или библиотеки.

Система государственного надзора и контроля в области персональных данных

Схематично система государственного надзора и контроля в области персональных данных представленная на рис.3. Видно, что надзор и контроль осуществляют 3 органа:

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

Если ФСБ и ФСТЭК специализируются на вопросах информационной безопасности в целом, то Роскомнадзор специализируется исключительно на вопросах персональных данных. **Роскомнадзор —** это уполномоченный федеральный орган исполнительной власти по защите прав субъектов ПД и действует на основании постановления Правительства РФ от 16.03.2009 № 228 «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций». Иначе говоря, ФСБ и ФСТЭК в первую очередь проверяют, какие меры приняты по защите персональных данных; Роскомнадзор оценивает, не нарушают ли организации прав граждан, связанных с законодательством по персональным данным, поэтому все жалобы граждан на несоблюдение 152-ФЗ поступают именно в Роскомнадзор.

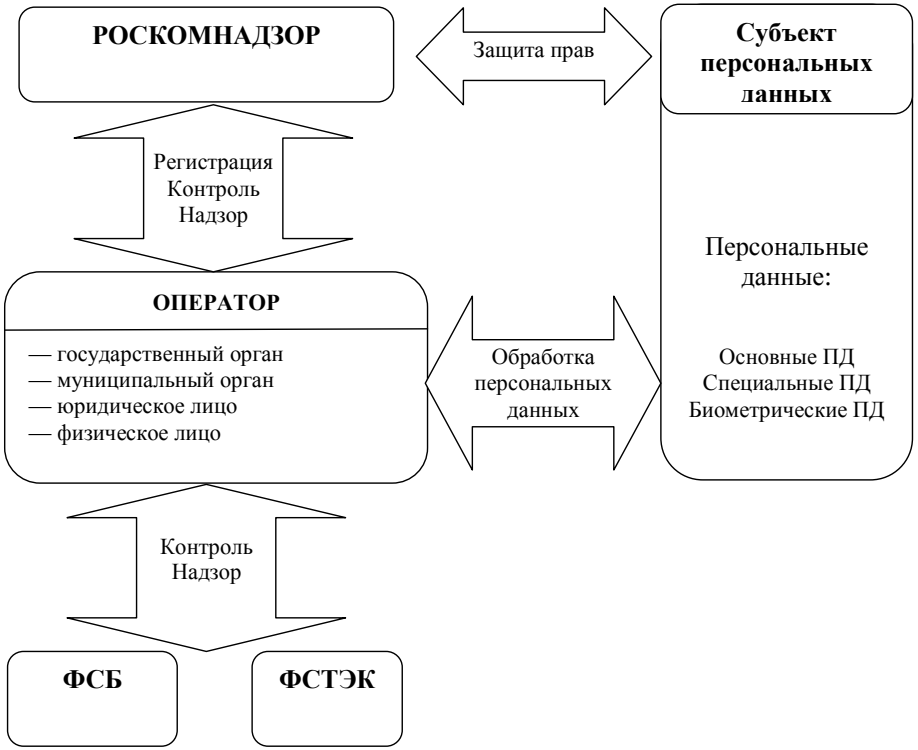

Рис. 3. Система государственного надзора в области персональных данных

Поскольку область использования персональных данных крайне широка, то можно сделать вывод, что оператором персональных данных является практически любое юридическое лицо (вне зависимости от формы собственности), государственные органы, а также физические лица (если они являются индивидуальными предпринимателями или при решении каких-нибудь задач используют чужие персональные данные). Роскомнадзор, кроме надзорной, имеет еще и функцию регистрации операторов персональных данных. Обязанностью вести реестр операторов он обладает как уполномоченный орган по защите прав субъектов персональных данных согласно п. 3 ч. 5 ст. 23 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

На рис.4 видна динамика роста числа операторов персональных данных в реестре Роскомнадзора. С января 2008 по июнь 2011 г. в реестре зарегистрировались почти 170 000 учреждений, из них 100 000 пришлись

на 2009 г. На 14 июля 2012 г. количество зарегистрированных операторов составляет 259 757 организаций.

Рис. 4. Динамика роста числа операторов персональных данных в реестре Роскомнадзора

Несмотря на кажущееся большим количество операторов, большинство коммерческих организаций не подали информацию о себе в реестр операторов персональных данных. Этот вывод можно сделать, проанализировав количество государственных учреждений в России, подавших данные в реестр «по приказу». В России — около 100 тыс. только образовательных учреждений (школ, детских садов, домов творчества, детских домов, интернатов и т.п.); если добавить библиотеки, поликлиники, собесы, подростковые клубы, то видно, что доля коммерческих структур чрезвычайно невысока, а ведь только число малых предприятий в России приближается к 1 млн.

В данном случае это никак не связано с бюрократическими барьерами. Для включения в реестр достаточно провести несложную процедуру — заполнить форму «Уведомление об обработке (о намерении осуществлять обработку) персональных данных» на сайте Роскомнадзора (рис.5). После заполнения формы и отправки ее в информационную систему Роскомнадзора оператору необходимо распечатать заполненную форму, после чего ее подписать и направить в соответствующий территориальный орган Роскомнадзора по месту регистрации оператора.

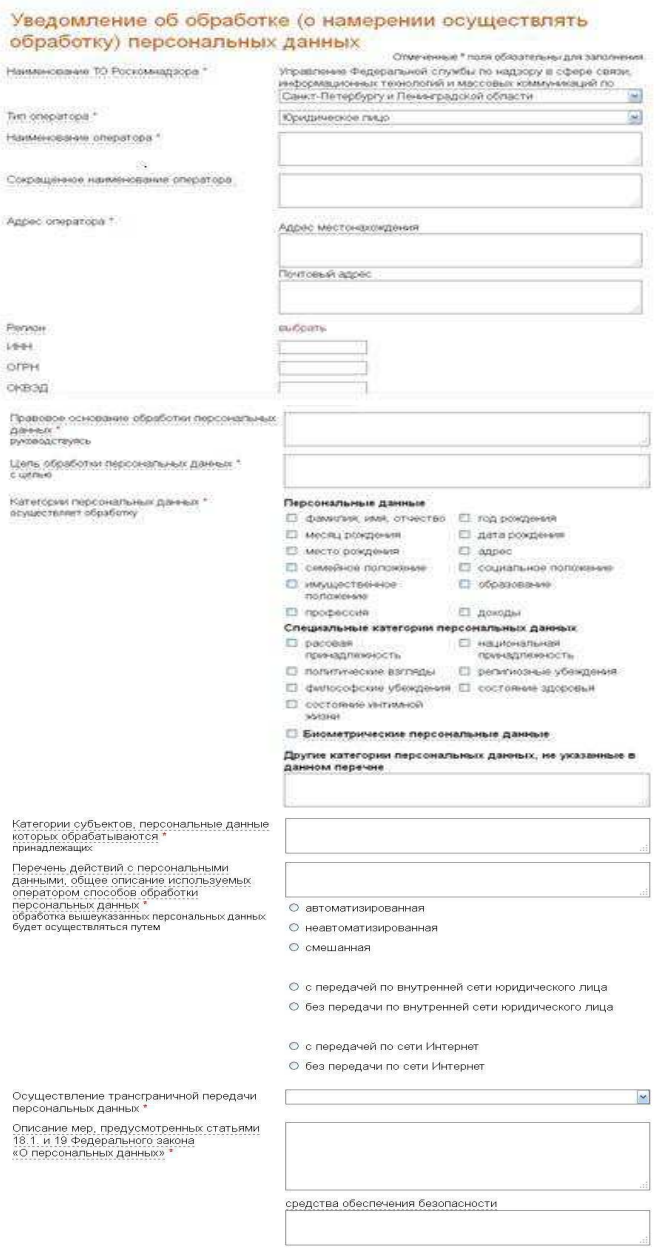

Рис. 5. Форма уведомления Роскомнадзора

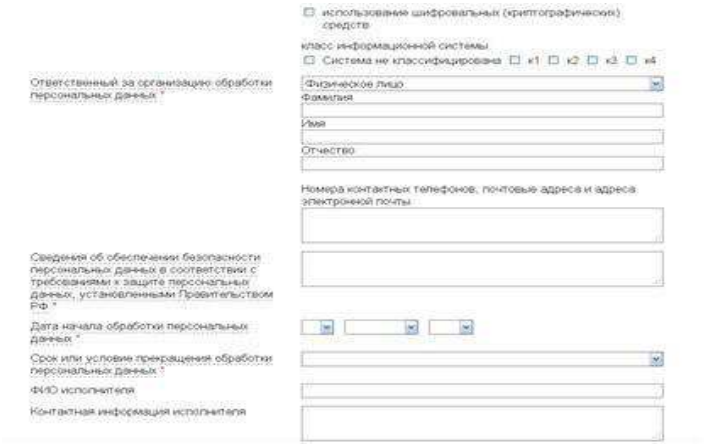

Рис. 5. Форма уведомления Роскомнадзора (продолжение)

Заполнение формы уведомления об обработке персональных данных

Рассмотрим подробнее принцип заполнения полей в данной форме. В первую группу полей вводятся общие данные об операторе персональных данных – это полное и сокращенное наименование по уставу, юридический и почтовый адрес, ИНН, ОГРН и т.п.

Следующие два поля уже несут серьезную смысловую нагрузку. В поле «Правовое основание обработки персональных данных» вводятся все нормативные документы, на основании которых, оператор обрабатывает персональные данные. В качестве примера рассмотрим, как это поле заполняется государственными образовательными учреждениями (школа, гимназия) Санкт-Петербурга. Пример взят из формы, заполненной в ноябре 2012 г. и одобренной Роскомнадзором:

«…руководствуясь федеральным законом от 30.12.2001 №197-ФЗ «Трудовой кодекс Российской Федерации» (с изменениями на 28 июля 2012г.), статьями 85-90; законом Российской Федерации от 10.07.1992 №3266-1 «Об образовании» (с изменениями на 10 июля 2012г.); федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (с изменениями на 25 июля 2011г.); приказом Министерства образования и науки Российской Федерации от 15.02.2012 №107 «Об утверждении порядка приема граждан в общеобразовательные учреждения»; постановлением Правительства Санкт-Петербурга от 17.02.2009 №149 «О мерах по реализации закона Санкт-Петербурга “Об общем образовании”»; постановлением Правительства Санкт-Петербурга от 04.06.2009 №655 «О мерах по реализации закона Санкт-Петербурга “О дополнительных мерах социальной поддержки отдельных категорий граждан в части предоставления на льготной основе питания в образовательных учреждениях Санкт-Петербурга”» (с изменениями на 23

марта 2011г.); распоряжением Комитета по образованию Санкт-Петербурга от 21.08.2006 №869-р «О внедрении автоматизированной информационной системы учета детей школьного возраста в образовательных учреждениях Санкт-Петербурга "Параграф-движение"»; распоряжением Комитета по транспорту Санкт-Петербурга от 27.06.2007 №31-р «О видах проездных билетов и порядке их обращения» (с изменениями на 27 января 2012г.); распоряжением Комитета по образованию Санкт-Петербурга от 08.06.2009 «О мерах по реализации постановления Правительства Санкт-Петербурга от 04.09.2009 №655»; распоряжением Комитета по образованию Санкт-Петербурга от 10.09.2010 «О внедрении комплексной автоматизированной информационной системы каталогизации ресурсов образования»; уставом ОУ, утвержденным распоряжением КО № ____ от _____»…

Как видно из примера, ведение бюджетной организации ИСПДн, отличной от бухгалтерского и кадрового учета, должно основываться на федеральных, региональных или муниципальных нормативных документах.

Поле «Цель обработки персональных данных» чаще всего заполняется следующим образом: *«с целью ведения профессиональной деятельности работников»*.

Следующее поле «Категории персональных данных» состоит из 2 частей. В первой можно выбрать, какие данные обрабатываются, причем сделать это по категориям: персональные данные, специальные персональные данные, биометрические персональные данные, а во второй — дописать обрабатываемые в ИСПДн данные, не упомянутые в первой части.

В поле «Категории субъектов, персональные данные которых обрабатываются, принадлежащих» чаще всего ставится — «работникам учреждения». Если в ИСПДн хранятся еще и другие персональные данные, через запятую перечисляются эти категории субъектов.

Очень важным является следующее обязательное для заполнения поле: «Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных». Бытует мнение, что если оператор может только просматривать данные, то, следовательно, никакой обработки персональных данных не ведется. На самом деле это не так. Чаще всего в качестве ответа надо ставить полный набор операций: *«сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), уничтожение персональных данных»*. Как видим, в перечне есть вариант «использование». Он как раз и означает, что даже только просматривая персональные данные, компания становится оператором.

Следующие четыре пункта очень важны. Ответы выбираются из вариантов, предложенных в форме. Выбираются они в соответствии с актом классификации ИСПДн, правила заполнения которого мы рассмотрим ниже.

В оставшихся вопросах часть относится к организационным моментам. Это — ФИО ответственного за обработку персональных данных, его контакты; ФИО и контакты лица, заполнившего анкету. В качестве даты начала обработки персональных данных ставится дата регистрации учреждения, если нет иных документов, регламентирующих начало работ с ПДн.

Сложности могут возникнуть с пунктом «Описание мер, предусмотренных статьями 18.1 и 19 федерального закона "О персональных данных"». Минимальный набор мер, описывающийся в данном пункте, будет выглядеть так: *«Разработаны локальные акты, регламентирующие обработку персональных данных, в которых определены лица, допущенные к работе с персональными данными; правила доступа к персональным данным; регистрация и учет всех действий, совершаемых с персональными данными в информационной системе. Создана модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Осуществляется административный контроль за принимаемыми мерами по обеспечению безопасности»*. Подробнее о всех принятых мерах и разработанных документах мы поговорим в 5 главе пособия.

Еще один сложный пункт — это «Сведения об обеспечении безопасности персональных данных». Ответ на него делится на две части: одна — об автоматизированной обработке данных, вторая — о ручной обработке. Если оператор использует только один вид обработки данных, ему в этом поле надо отвечать только о том виде обработки, которую он использует (ручная, автоматическая). Ниже приведен пример (также из одобренного Рокомнадзором уведомления), из которого видно, что на постановление 1119 ссылаются при автоматизированной обработке персональных данных, а на постановление 687— если речь идет о ручной обработке.

В соответствии с постановлением Правительства РФ от 01.11.2012 №1119 разработаны локальные акты, в которых

- указан перечень лиц, которые допущены к персональным данным, обрабатываемым в информационной системе, необходимым для выполнения ими служебных (трудовых) обязанностей;
- определен режим обеспечения безопасности помещений, в которых размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях

лиц, не имеющих права доступа в эти помещения: журналы учета, парольная защита;

– определены места хранения носителей персональных данных.

В соответствии с постановлением Правительства РФ от 15.09.2008 №687:

1) разработаны локальные акты, в которых указан: перечень мер, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ; перечень лиц, ответственных за реализацию указанных мер;

2) обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

Нам осталось только разобрать блок вопросов о «средствах обеспечения безопасности». Если у организации имеется техническая защита ИСПДн и используется шифрование, то при заполнении данного раздела может помочь представитель фирмы подрядчика, обладающей лицензией ФСБ или ФСТЭК и выполняющий заказ на данные работы. Например, большинство представителей бюджетных учреждений не смогут правильно проставить уровень криптографической защиты персональных данных. Если же криптографической защиты нет, то остается проставить только класс ИСПДн, как определить который мы будем сейчас разбирать.

Классификации информационной системы персональных данных

Для проведения классификации информационной системы персональных данных используют многошаговый алгоритм [3].

1. На первом шаге анализируют значения обрабатываемых персональных данных. Это могут быть ФИО, адрес, дата рождения, № паспорта, ИНН и др. используемые в информационной системе. В соответствии со значениями данных им назначается категория персональных данных, обрабатываемых в информационной системе ($X_{пд}$):

– категория 1 — персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

– категория 2 — персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

– категория 3 — персональные данные, позволяющие идентифицировать субъекта персональных данных;

– категория 4 — обезличенные и (или) общедоступные персональные данные.

2. На втором шаге оценивается объём обрабатываемых персональных данных ($X_{пдн}$) и количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе. $X_{пдн}$ определяется

– если в информационной системе одновременно обрабатываются персональные данные более чем 100 тыс. субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;

– если в информационной системе одновременно обрабатываются персональные данные от 1 до 100 тыс. субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;

– если в информационной системе одновременно обрабатываются данные менее чем 1 тыс.субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

3. Следующим шагом определяется, относится ли информационная система персональных данных (по заданным оператором характеристикам безопасности) к типовым или специальным.

Типовые информационные системы — системы, в которых требуется обеспечение только конфиденциальности персональных данных.

Специальные информационные системы — системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

К специальным информационным системам должны быть отнесены системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных; системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интерес).

4. На следующем шаге определяется, является ли ИСПДН автономной или распределенной. ИСПДн делятся на

– автономные (не подключенные к иным информационным системам) комплексы технических и программных средств, предназначенные для обработки персональных данных (автоматизированные рабочие места);

– комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные информационные системы);

– комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).

5. Пятым шагом становится определение наличия подключений к сетям связи общего пользования и (или) сетям международного информационного обмена. Имеются в виду общедоступные системы обмена, не имеющие специальных средств защиты информации, и ИНТЕРНЕТ.

6. На шестом шаге определяется, однопользовательский или многопользовательский режим обработки персональных данных используется в информационной системе.

7. На седьмом шаге определяется, есть или нет в системе разграничение прав доступа пользователей.

8. Последним восьмым шагом мы определяем местонахождение информационных систем персональных данных

– в пределах Российской Федерации;

– частично за пределами Российской Федерации;

– целиком за пределами Российской Федерации.

По результатам анализа исходных данных типовой информационной системе присваивается один из следующих классов:

– класс 1 (К1) — информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;

– класс 2 (К2) — информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;

– класс 3 (К3) — информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;

– класс 4 (К4) — информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

Класс типовой информационной системы определяется в соответствии с табл.1.

Данный алгоритм определяется одновременным приказом ФСБ, ФСТЭКа и Роскомнадзора от 13 февраля 2008 г. № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных».

Таблица 1. Определение класса ИСПДн

$\frac{X_{НПД}}{X_{ПД}}$	3	2	1
Категория 4	К4	К4	К4
Категория 3	К3	К3	К2
Категория 2	К3	К2	К1
Категория 1	К1	К1	К1

Многие операторы ПДн увлекаются анонимизацией (обезличиванием) персональных данных для минимизации класса ИСПДн или вообще ухода из-под действия закона. Один из практикуемых подходов заключается в том, что из баз данных ИСПДн, используемых в организации, удаляется информация, позволяющая идентифицировать субъектов (чаще всего это — их ФИО) и заменяется неким абстрактным идентификатором. Данный идентификатор вместе с ФИО и прочими данными, позволяющими однозначно идентифицировать субъекта, хранится в службе каталогов (например, в AD), которая и классифицируется как ИСПДн. Все же прочие ИСПДн организации (по мнению оператора) — вовсе ИСПДн и не являются (или относятся к четвертому классу согласно принятой на данный момент в РФ классификации, что по факту — то же самое).

Подобные "анонимизаторы" обманывают сами себя, т.к. то, чем они занимаются (с точки зрения развитой европейской судебной практики), это — не обезличивание, а всего лишь разнесение персональных данных по нескольким базам данных. Подобные действия могут иметь смысл сами по себе (с точки зрения защиты и обработки ПДн), но, к сожалению, не позволяют обезличить данные. В этом случае европейские директивы, например, признают субъекта идентифицируемым, если это можно сделать любыми доступными оператору (или любому другому лицу) способами. Очевидно, что оператор ПДн располагает и необходимыми полномочиями и техническими возможностями для определения того, кому принадлежат обрабатываемые им данные, даже если они разнесены по разным базам данных. Например, банк, имитировавший кредитную карту, сможет (по данным на

карте) определить, кому она принадлежит, независимо от того, как он хранит эти данные (вместе или по отдельности) и как обеспечивает защиту этих данных. Оператор сотовой связи по номеру телефона имеет возможность определить, кто является абонентом и т.д.

Контрольные вопросы

1. Должно ли регистрироваться как оператор персональных данных государственное автономное учреждение «Музей современного искусства»?
2. Какие надзорные органы осуществляют контроль над операторами персональных данных?
3. В главе написано, что 260 000 зарегистрированных операторов персональных данных — это крайне мало. Определите, будет ли достаточным (согласно 152 ФЗ) число операторов ПДн в количестве 650 000.
4. Определите, типовой или специальной ИСПДн будет являться АИС «Паспорт здоровья». Обоснуйте ответ.

Глава 4.
Методика определения актуальных угроз безопасности персональных данных

Методика предназначена для использования при проведении работ по обеспечению безопасности персональных данных при их обработке в следующих автоматизированных информационных системах персональных данных:

- государственных или муниципальных ИСПДн;
- ИСПДн, создаваемых и (или) эксплуатируемых предприятиями, организациями и учреждениями (далее – организациями) независимо от форм собственности, необходимых для выполнения функций этих организаций в соответствии с их назначением;
- ИСПДн, создаваемых и используемых физическими лицами, за исключением случаев, когда последние используют указанные системы исключительно для личных и семейных нужд.

Под угрозами безопасности ПДн при их обработке в ИСПДн понимается совокупность условий и факторов, создающих опасность несанкционированного (в том числе случайного) доступа к персональным данным, результатом которого может стать

- уничтожение,
- изменение,
- блокирование,
- копирование,
- распространение персональных данных,
- иные несанкционированные действия в отношении персональных данных при их обработке в информационной системе персональных данных.

Угрозы безопасности ПДн могут быть реализованы за счет утечки ПДн

- по техническим каналам (утечка информации, обрабатываемой в технических средствах ИСПДн; перехват информации при ее передаче по каналам связи; утечка акустической (речевой) информации);
- за счет несанкционированного доступа с использованием соответствующего программного обеспечения.

Детальное описание угроз, связанных с утечкой ПДн по техническим каналам, приводится в «Модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

Выявление технических каналов утечки ПДн осуществляется на основе нормативных и методических документов ФСТЭК России.

Источниками угроз, реализуемых за счет несанкционированного доступа к базам данных с использованием штатного или специально разработанного программного обеспечения, являются субъекты, действия которых нарушают регламентируемые в ИСПДн правила разграничения доступа к информации.

Этими субъектами могут быть:

- нарушитель;
- носитель вредоносной программы;
- аппаратная закладка.

Под нарушителем здесь и далее понимается физическое лицо (лица), случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности ПДн при их обработке техническими средствами в информационных системах. С точки зрения наличия права легального доступа в помещения, в которых размещены аппаратные средства, обеспечивающие доступ к ресурсам ИСПДн, нарушители подразделяются на два типа:

1) нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена, – *внешние* нарушители;
2) нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн, – *внутренние* нарушители.

Выявление угроз НСД к ПДн, реализуемых с применением программных и программно-аппаратных средств, осуществляется на основе экспертного метода, в том числе путем опроса специалистов, персонала ИСПДн, должностных лиц. При этом могут использоваться сетевые сканеры для подтверждения наличия и выявления уязвимостей программного и аппаратного обеспечения ИСПДн. Для проведения опроса составляются специальные опросные листы.

Наличие источника угрозы и уязвимого звена, которое может быть использовано для реализации угрозы, свидетельствует о наличии данной угрозы. Формируя на основе опроса перечень источников угроз ПДн, на основе опроса и сетевого сканирования — перечень уязвимых звеньев ИСПДн, а также по данным обследования ИСПДн — перечень технических каналов утечки информации, определяются условия существования в ИСПДн угроз безопасности информации и составляется их полный перечень. На основании этого перечня в соответствии с описанным ниже порядком формируется перечень актуальных угроз безопасности ПДн.

Порядок определения актуальных угроз безопасности персональных данных в информационных системах персональных данных

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн. Подход к составлению перечня актуальных угроз состоит в следующем.

Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности ИСПДн и частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в табл.2.

Таблица 2. Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	высокий	средний	низкий
1. По территориальному размещению			
Распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом	-	-	+
Городская ИСПДн, охватывающая не более одного населенного пункта (города)	-	-	+
Корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации	-	+	-
Локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий	-	+	-
Локальная ИСПДн, развернутая в пределах одного здания	+	-	-
2. По наличию соединения с сетями общего пользования			
ИСПДн, имеющая многоточечный выход в сеть общего пользования	-	-	+
ИСПДн, имеющая одноточечный выход в сеть общего пользования	-	+	-
ИСПДн, физически отделенная от сети общего пользования	+	-	-
3. По встроенным (легальным) операциям с записями баз персональных данных			
Чтение, поиск	+	-	-
Запись, удаление, сортировка	-	+	-
Модификация, передача	-	-	+
4. По разграничению доступа к персональным данным			
ИСПДн, к которой доступ имеют определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ИСПДн	-	+	-
ИСПДн, к которой доступ имеют все сотрудники организации, являющейся владельцем ИСПДн	-	-	+
ИСПДн с открытым доступом	-	-	+

5. По наличию соединений с другими базами ПДн иных ИСПДн			
Интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн)	-	-	+
ИСПДн, в которой используется одна база ПДн, принадлежащая организации-владельцу ИСПДн	+	-	-
6. По уровню обобщения (обезличивания) ПДн			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными	+	-	-
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации	-	+	-
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными	-	-	+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки			
ИСПДн, предоставляющая всю базу данных с ПДн	-	-	+
ИСПДн, предоставляющая часть ПДн	-	+	-
ИСПДн, не предоставляющая никакой информации	+	-	-

Исходная степень защищенности определяется следующим образом.

– ИСПДн имеет *высокий* уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные — среднему уровню защищенности (положительные решения по второму столбцу).

– ИСПДн имеет *средний* уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительных решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.

– ИСПДн имеет низкую степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент:

0 — для высокой степени исходной защищенности;

5 — для средней степени исходной защищенности;

10 — для низкой степени исходной защищенности.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько

вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки.

Маловероятно — отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся).

Низкая вероятность — объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации).

Средняя вероятность — объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны.

Высокая вероятность — объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент:

0 — для маловероятной угрозы;

2 — для низкой вероятности угрозы;

5 — для средней вероятности угрозы;

10 — для высокой вероятности угрозы.

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением $Y = (Y1+Y2)/20$.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

если $0<=Y<=0.3$, то возможность реализации угрозы признается низкой;

если $0.3<Y<=0.6$, то возможность реализации угрозы признается средней;

если $0.6<Y<=0.8$, то возможность реализации угрозы признается высокой;

если $0.8<Y$, то возможность реализации угрозы признается очень высокой.

Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИСПДн.

Этот показатель имеет три значения:

1) **низкая опасность** — если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

2) **средняя опасность** — если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
3) **высокая опасность** — если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами, приведенными в табл.3.

Таблица 3. Правила отнесения угрозы безопасности ПДн к актуальной

Возможность реализации угрозы	Показатель опасности угрозы		
	низкая	средняя	высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

С использованием данных о классе ИСПДн и составленного перечня актуальных угроз, на основе «Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и «Основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» формулируются конкретные организационно-технические требования по защите ИСПДн от утечки информации по техническим каналам от несанкционированного доступа и осуществляется выбор программных и технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации ИСПДн.

Постановление правительства № 1119

Рассмотрим некоторые особенности постановления Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

В постановлении вводятся 4 уровня защищенности ПДн при их обработке в ИСПДн (1 — максимальные требования, 4 — минимальные);

В документе вводится определение актуальности угроз (но не самих типов угроз) 1-го, 2-го и 3-го типов;

Актуальный тип угроз определяет оператор с учетом совокупности условий, факторов и оценки вреда (прорыв в том, что в явном виде модель угроз не требуется. В тоже время МУ вполне допустима на этом этапе);

В постановлении №1119 ИСПДн разбиты на 4 типа:

1) ИСПДн обрабатывает специальные категории ПДн (ИСПДн-С);
2) ИСПДн обрабатывает биометрические ПДн (ИСПДн-Б);

3) ИСПДн обрабатывает общедоступные ПДн (ИСПДн-О);
4) ИСПДн обрабатывает иные категории ПДн (ИСПДн-И).

Уровень защищенности определяется согласно табл.4.

Таблица 4. Правила определения уровня защищенности ИСПДн [2]

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1	2	3
ИСПДн-С	Не сотрудников	Более 100 тыс.	УЗ 1	УЗ 1	УЗ 2
		Менее 100 тыс.	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Любое	УЗ 1	УЗ 2	УЗ 3
ИСПДн-Б	Не сотрудников	Более 100 тыс.	УЗ 1	УЗ 2	УЗ 3
		Менее 100 тыс.	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Любое	УЗ 1	УЗ 2	УЗ 3
ИСПДн-И	Не сотрудников	Более 100 тыс.	УЗ 1	УЗ 2	УЗ 3
		Менее 100 тыс.	УЗ 1	УЗ 3	УЗ 4
	Сотрудников	Любое	УЗ 1	УЗ 3	УЗ 4
ИСПДн-О	Не сотрудников	Более 100 тыс.	УЗ 2	УЗ 2	УЗ 4
		Менее 100 тыс.	УЗ 3	УЗ 3	УЗ 4
	Сотрудников	Любое	УЗ 4	УЗ 3	УЗ 4

В зависимости от уровня защищенности необходимо выполнять следующие общие требования, в соответствии с табл.5.

Таблица 5. Требования к защите ПДН в зависимости от уровня защищенности [2]

Требования к защите ПДн в зависимости от уровня защищенности	УЗ 4	УЗ 3	УЗ 2	УЗ 1
Технические средства защиты				
Применение средств защиты информации в соответствии с актами ФСТЭК и ФСБ России (будут разрабатываться)	+	+	+	+
Применение средств защиты успешно прошедших процедуру оценки соответствия в соответствии с законодательством РФ	-	-	+	+
Организационные и другие технические меры				
Организация режима обеспечения безопасности помещений, в которых размещена ИСПДн, исключающего возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц	+	+	+	+
Обеспечение сохранности носителей персональных данных	+	+	+	+

Руководитель оператора утверждает документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения ими служебных обязанностей	+	+	+	+
Руководитель оператора назначает должностное лицо, ответственное за обеспечение безопасности персональных данных в ИСПДн	-	+	+	+
Обеспечение доступа к содержанию электронного журнала сообщений только должностному лицу оператора или уполномоченному лицу	-	+	+	+
Обеспечение регистрации факта изменения полномочий субъектов доступа к объектам доступа автоматизированными средствами ИСПДн в электронном журнале безопасности	-	-	-	+
Руководитель оператора назначает структурное подразделение, ответственное за обеспечение безопасности персональных данных в ИСПДн	-	-	-	+

Контрольные вопросы

1. Кто является источниками угроз, реализуемых за счет несанкционированного доступа к базам данных с использованием штатного или специально разработанного программного обеспечения?
2. На какие группы делятся технические и эксплуатационные характеристики ИСПДн?
3. Какие числовые коэффициенты ставятся в соответствие степени исходной защищенности при составлении перечня актуальных угроз безопасности ПДн?
4. По каким значениям коэффициента реализуемости угрозы *Y* формируется вербальная интерпретация реализуемости угрозы?

Глава 5.
Основные мероприятия по обеспечению безопасности персональных данных в государственных учреждениях

Начиная с 2006 г. согласно 152 ФЗ «О защите персональных данных» любое государственное учреждение является оператором персональных данных. С этим сложно спорить, поскольку любая организация хранит у себя персональные данные сотрудников и не только хранит, но и ведет автоматизированную обработку этих данных.

Например, в Санкт-Петербурге во всех общеобразовательных ОУ имеется АИС «Параграф» с помощью, которой и ведется данная обработка, но на самом деле автоматизированная обработка персональных данных ведется и в тех регионах, в которых системы управления учреждениями еще не внедрены повсеместно, поскольку с точки зрения проверяющего органа, которым в данном случае является Роскомнадзор, ввод списка персональных данных с помощью текстового редактора, тоже является автоматизированной обработкой персональных данных.

Если же разбирать ситуацию более пристально, то мы увидим, что практически в каждом государственном учреждении есть еще и информация о получателях услуг. В образовательном учреждении — это информация об учащихся и их родителях (с паспортными данными, местом проживания, местом работы, контактными телефонами), всегда заполнявшаяся на последних страницах классных журналов, а сейчас без раздумий переносящаяся в автоматизированные системы; в поликлиниках — данные о пациентах, в библиотеках — о читателях и т.п.

Рис. 6. Мероприятия по защите персональных данных

Мероприятия по защите персональных данных можно разделить на два больших сегмента (рис. 6).

Технические работы должны проводится только фирмами, имеющими лицензию ФСТЭК или ФСБ на проведение подобного типа работ.

В то же время необходимо отметить, что в ряде случаев, когда класс ИСПДн определен как 3-й или согласно распоряжению №1119 требуемый уровень защищенности — 4, учреждение может ограничиться организационными мероприятиями. Как мы увидим, это не означает, что ничего не надо делать, но позволяет сэкономить значительные финансовые средства, что крайне важно в условиях бюджетного финансирования. В данном пособии мы рассмотрим только необходимые организационные меры и перечень необходимых документов.

Организационные мероприятия по обеспечению безопасности персональных данных

Ниже приведен примерный перечень документов, которые необходимо разработать любому государственному учреждению. Конечно, этот список может быть расширен, но в некоторых случаях все 28 ниже перечисленных документов не требуются.

1. Приказ о назначении ответственного за обработку ПДн (персональных данных).
2. Приказ о назначении ответственных лиц за ПДн и список ответственных лиц.
3. Приказ о введении режима обработки ПДн.
4. Приказ о создании комиссии для классификации ИСПДн.
5. Список подсистем в которых обрабатываются персональные данные.
6. Перечень сотрудников допущенных к работе с персональными данными.
7. Перечень сотрудников допущенных к обработке персональных данных.
8. Перечень персональных данных с местами хранения, обработки и списком допущенных лиц.
9. Перечень защищаемой информации.
10. Положение по обработке персональных данных.
11. Положение о разграничении прав доступа к обрабатываемым персональным данным в информационных системах.
12. Частная модель угроз.
13. Акт классификации ИСПДн.

14. Матрица доступа в подсистему ИСПДн.
15. Заключение о возможности ввода в эксплуатацию средств СЗИ ИСПДн.
16. Акт об уничтожении персональных данных.
17. Инструкция по организации парольной защиты.
18. Инструкция по антивирусной защите.
19. Инструкция по обработке персональных данных без использования средств автоматизации.
20. Инструкция по обеспечению безопасности персональных данных обрабатываемых в информационной системе персональных данных.
21. Инструкция ответственного за СЗИ ИСПДн.
22. Согласие на обработку ПДн.
23. Обязательство о неразглашении ПДн.
24. Журнал учета технической и эксплуатационной документации.
25. Журнал учета средств защиты СЗИ ИСПДн.
26. Журнал учета пользователей ИСПДн, прошедших обучение правилам работы со средствами СЗИ.
27. Журнал учета обращений субъектов ПДн в ИСПДн.
28. Журнал учета носителей, предназначенных для хранения ПДн.

Видно, что перечисленные документы делятся на несколько групп. Рассмотрим подробнее каждую группу.

1-я группа (документы 1 — 4) это приказы по учреждению. Самый важный из приказов — о назначении ответственного за обработку персональных данных (или, как мы называли его до июля 2011 г., — ответственного за безопасность ПДн). Одна из типичных ошибок администрации учреждения — назначить на эту должность инженера. Но работа по организации обработки ПДн — это работа не столько с техникой, сколько с документами и людьми, а, значит, разумнее, чтобы отвечал за нее заместитель руководителя. Оптимально, когда это вменяют заместителю директора, а технический специалист является его помощником. Это обусловлено тем, что именно заместитель директора (а то — и только сам директор), владеет информацией о том, кто из сотрудников с какими персональными данными и с какими ИСПДн работает.

После выпуска первого приказа ответственный или созданная рабочая группа готовят вышеперечисленный набор документов, начиная с оставшихся приказов.

Часто вызывает вопрос, чем приказ о назначении ответственных лиц за ПДн и список ответственных лиц отличается от первого приказа. Суть отличия в том, что в первом случае назначается ответственный за режим безопасности, а во втором приказе — ответственные непосредственно за сами персональные данные. Соответственно разные люди могут отвечать за разные данные. Например, в библиотеке за личные дела сотрудников будет отвечать руководитель кадровой службы, а за персональные данные читателей — руководитель отдела обслуживания.

Приказы 3 и 4 — достаточно простые, и вопросов у разработчиков документов не вызывают.

2-я группа (документы 5 — 8) — перечни подсистем данных сотрудников. Рассмотрим каждый из документов подробнее.

Список подсистем, в которых обрабатываются персональные данные — это документ, в котором перечислены все информационные системы, имеющиеся в организации, в которых идет обработка персональных данных. Это могут быть разные программные продукты, а могут быть модули общей информационной системы предприятия. В данном случае важно, не какая программа, а какие данные. Так, у организации бухгалтерский учет и учет клиентов могут вестись в 2 разных программных комплексах, а могут при помощи системы 1С Предприятие. В любом случае в списке подсистем будут две разных строки — подсистема кадры и подсистема клиенты.

Перечень сотрудников, допущенных к работе с персональными данными, — это документ, в котором перечисляются фамилии и должности тех сотрудников, которые имеют доступ к персональным данным

Перечень сотрудников, допущенных к обработке персональных данных, это — документ, по названию очень похожий на предыдущий, однако в данный перечень будут входить только те сотрудники, которые имеют право менять персональные данные. Например, оператор call-центра видит персональные данные клиентов, но не имеет право их менять, а значит, попадет в шестой документ, но не попадет в седьмой.

Если предыдущие два перечня имели доступ в ИСПДн со стороны пользователей, то перечень персональных данных с местами хранения, обработки и списком допущенных лиц рассматривает этот вопрос с другой стороны. В данном перечне указывается, на каком сервере (физическое размещение) и в какой программе находятся персональные данные, и какие сотрудники к этим данным имеют доступ. В предыдущем документе мы говорили, что руководитель call-центра Иванов имеет право на чтение персональных данных сотрудников и редактирование персональных данных клиентов. Теперь мы пишем, что персональные данные клиентов находятся на сервере баз данных учреждения в CRM-системе «Парус», смотреть их могут операторы call-центра Петров, Сидорова и Каспарчук,

читать и редактировать может директор call-центра Иванов, а читать, редактировать, добавлять и удалять — руководитель отдела продаж Георгиев и системный администратор Кравцова.

Последний документ из данной группы — перечень защищаемой информации. В него входят только защищаемые персональные данные, иначе говоря, все данные, кроме общедоступных.

Большой минус данной группы документов, что при любых кадровых изменениях их необходимо переделывать.

3-я часть (документы 9 — 12) — это положения и частная модель угроз. Эти документы разрабатываются один раз и надолго. Существенные изменения в них вносят только в случае добавления ИСПДн или серьезных изменений в организационной структуре учреждения. Положения и частная модель угроз разрабатываются в соответствии с образцами, спускаемыми из региональных министерств, занимающихся информационными технологиями.

4-я группа (документы 13 — 16) является одной из самых важных в нашем списке. Именно в данной группе находится акт классификации ИСПДн, алгоритм принятия, которого мы разбирали в главе 3. Документ «матрица доступа в подсистему ИСПДн» представляет собой двумерную таблицу, где для подсистемы расписаны какие специалисты, какие имеют права при работе с подсистемой. Это может выглядеть как в табл.6.

Таблица 6. Матрица доступа

Должность	Чтение	Редактирование	Добавление	Удаление
Консультант	+	-	-	-
Начальник Call-центра	+	+	-	-
Системный администратор	+	+	+	+
Заместитель директора	+	+	+	-

Из таблицы видно, что тут не прописываются конкретные фамилии, а матрица привязана к должностям. Таким образом, при смене сотрудника, работающего с персональными данными (например, придет новый консультант или даже системный администратор), менять этот документ нет необходимости.

Еще одной особенностью данного документа является, то, что он делается отдельно для каждой подсистемы персональных данных. Если у ИСПДн две подсистемы (кадры и клиенты), то делаются две матрицы доступа, а если подсистем пять, то и матриц доступа тоже будет пять.

Акт об уничтожении персональных данных нужен, если организация не должна хранить персональные данные годами. В этом случае составляется акт по форме, и устаревшие данные уничтожаются.

Заключение о возможности ввода в эксплуатацию средств СЗИ ИСПДн дает фирма, поставляющая организации сертифицированные средства.

5-я группа (документы 17 — 21) это набор инструкций. Эти документы аналогичны 3-й группе. Тоже разрабатываются по образцам и долго остаются без изменений. Необходимо отметить, что инструкции 17 и 18 относятся не только к защите персональных данных, они должны учитываться и при других работах по обеспечению информационной безопасности.

6-я группа (документы 22 и 23) состоит всего из двух документов, но зато требует большого объема организационной работы. Эти документы — согласие на обработку персональных данных и обязательство о неразглашении персональных данных. После того как эти документы разработаны, согласие необходимо взять у всех субъектов персональных данных — работников, получателей услуг и (или) их законных представителей. Обязательство о неразглашении подписывается всеми сотрудниками учреждения, работающими с персональными данными. Все согласия и обязательства собирают и хранят в бумажном виде в соответствующих папках, и их предъявляют проверяющим органам при необходимости.

7-я группа (документы 24 — 28) — журналы, которые должны вестись круглогодично.

Грамотно проведенная работа позволит не только подготовить необходимый комплект документов для возможной проверки, но и серьезно настроить сотрудников, работающих с персональными данными, ввести персонифицированную ответственность за эти данные. Как видим, организации недостаточно разово пригласить специалистов для разработки комплекта документов. Большая часть документации должна регулярно обновляться или еще более регулярно вестись специалистами, работающими с персональными данными.

С каждым годом все больше получателей услуг знают требования к защите персональных данных (и своих, и ребенка), а значит, государственное учреждение должно быть готово работать в ситуации жесткого прессинга по поводу автоматизированной обработки персональных данных со стороны общественности.

Контрольные вопросы

1. Кто должен быть лицом, ответственным за ПДн?
2. В каких группах есть документы, не меняющиеся при смене персонала в организации?
3. Сколько и каких журналов ведется в рассматриваемом нами комплекте документов?
4. С кого берется обязательство о неразглашении персональных данных?

Заключение

В заключение хочется отметить несколько особенностей данного методического пособия.

Во-первых, оно написано не для специалистов по информационной безопасности, а для работников бюджетных организаций. Прежде всего, оно рассчитано на тех, кто в государственных и муниципальных учреждениях назначен заниматься информационной безопасностью и при этом не имеет профильного образования, а зачастую (в школах, поликлиниках, библиотеках и т.п.) имеет высшее образование, но не технической направленности.

Во-вторых, это пособие является вторым из серии брошюр, написанных для данной аудитории и посвященных проблематике информационной безопасности. В работе освещены вопросы защиты персональных данных.

В-третьих, задачей работы было объяснить сложные вещи без описания серьезных технических и юридических особенностей, что возможно далеко не всегда.

Все вышеперечисленное позволяет надеяться, что методическое пособие будет полезно не только магистрантам направления «Управление государственными информационными системами», но и многочисленной категории «бюджетников», обязанных по долгу службы заниматься вопросами информационной безопасности.

Глоссарий

Анализ защищенности — процесс обнаружения уязвимостей ресурсов автоматизированной системы, а также выработка рекомендаций по их устранению.

Аттестация объекта — в информатизации деятельность по установлению соответствия комплекса организационно-технических мероприятий по защите объекта информатизации требованиям по безопасности информации.

Аудит — независимая проверка с целью выражения мнения о достоверности службы, задачей которой является проверка наличия адекватных мер контроля и сообщения руководству соответствующего уровня о несоответствиях.

Аудит безопасности (информации) — совокупность действий по независимой проверке и изучению документации автоматизированной информационной системы, а также по испытаниям средств защиты информации, направленная на обеспечение выполнения установленной политики безопасности информации и правил эксплуатации автоматизированной информационной системы, на выявление уязвимости данной системы и на выработку рекомендаций по устранению выявленных недостатков в средствах защиты информации, политике безопасности информации и правилах эксплуатации автоматизированной информационной системы.

Безопасность — качество или состояние защищенности от несанкционированного доступа или неконтролируемых потерь или воздействий.

Данные — информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека.

Доступ к информации — возможность получения информации и ее использования.

Информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных — информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без них.

Канал утечки информации — совокупность источника информации, средства и способа, используемого для реализации угрозы.

Модель угроз (безопасности информации) — физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Несанкционированное воздействие на информацию — воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Несанкционированный доступ к информации — доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Обладатель информации — лицо, самостоятельно создавшее информацию либо получившее (на основании закона или договора) право разрешать или ограничивать доступ к информации, определяемой по каким – либо признакам.

Оператор — государственный или муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание этой обработки.

Персональные данные — любая информация, относящаяся к определенному (или определяемому на основании такой информации) физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Пользователь — любая сущность (человек-пользователь или внешний объект ИТ) вне объекта оценки, которая взаимодействует с объектом оценки.

Пользователь информации — субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением.

Распространение информации — действие, направленное на получение информации неопределенным кругом лиц или передачу информации этому кругу лиц.

Санкционированный доступ — доступ к информации, не нарушающий правила разграничения доступа.

Собственник информации — субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами.

Угроза — совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба изделию ИТ или его владельцу.

Угроза безопасности информации — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Уничтожение информации — случайное или умышленное стирание информации на ее носителях при обработке техническими средствами, а также хищение носителей и технических средств.

Рекомендуемая литература

1. *Астахов А.* Как решаются вопросы персональных данных в цивилизованных странах? // Интернет портал ISO27000.RU. 2011. URL: http://iso27000.ru/blogi/aleksandr-astahov/kak-reshayutsya-voprosy-personalnyh-dannyh-v-civilizovannyh-stranah-chast-pervaya-chto-takoe-personalnye-dannye.
2. *Борисов С.* СЗПДн. Анализ. Проекты новых ПП РФ по защите ПДн 2 // Интернет блог ИБ на Кубани. 2012. URL: http://sborisov.blogspot.ru/2012/09/2.html.
3. *Галатенко В.А.* Основы информационной безопасности. М.: Интернет-университет информационных технологий. ИНТУИТ.ру. 2008.
4. Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных».
5. Постановление Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Приложение

Проект приказа

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ПРИКАЗ

«___»_____201__г. №_____

ОБ УТВЕРЖДЕНИИ СОСТАВА И СОДЕРЖАНИЯ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

В соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» (Собрание законодательства 2006, №31, ст.3451; 2009, №48, ст. 5716; №52, ст. 6439; 2010, №27, ст. 3407; №31, ст. 4173; ст. 4196; №49, ст. 6409; 2011, №23, ст. 3263; ст. 31, ст. 4701) и Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. №1085 (Собрание законодательства Российской Федерации, 2004, №34, ст. 3541; 2005, №13, ст. 1138; 2006, №49, ст. 5192; 2008, №43, ст. 4921; №47, ст. 5431; 2012, №7, ст. 818),

П Р И К А З Ы В А Ю:

1. Утвердить прилагаемые Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

2. Установить, что настоящий приказ применяется для обеспечения безопасности персональных данный во вновь создаваемых (модернизируемых) информационных системах персональных данных.

3. Признать утратившим силу приказ ФСТЭК России от 5 февраля 2010 г. №58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных».

Директор Федеральной службы
по техническому
и экспортному контролю В.СЕЛИН

УТВЕРЖДЕНЫ
приказом ФСТЭК России
от «__» _____ 2012 г. №___

СОСТАВ И СОДЕРЖАНИЕ
ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

(проект)

I. Общие положения

1. Настоящий документ разработан в соответствии с частью 4 статьи 19 Федерального закона «О персональных данных» (Собрание законодательства Российской Федерации 2006, №31, ст. 3451; 2009, №48, ст. 5716; №52, ст. 6439; 2010, №27, ст. 3407; №31, ст. 4173, ст. 4196; №49, ст. 6409; 2011, №23, ст. 3263; №31, ст. 4701) и устанавливает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее – информационные системы), принимаемых операторами для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2. В настоящем документе не рассматриваются вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, а также меры, связанные с применением шифровальных (криптографических) средств защиты информации.

3. Настоящий документ предназначен для выбора операторами информационных систем и (или) уполномоченными лицами организационных и технических мер по обеспечению безопасности персональных данных и их реализации в системе защиты персональных данных, создаваемой в соответствии с требованиями к защите персональных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119, в соответствии с установленным уровнем защищенности персональных данных.

Выбранные и реализованные в системе защиты персональных данных организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах должны обеспечивать нейтрализацию актуальных угроз безопасности

персональных данных, определенных в соответствии с частью 5 статьи 19 Федерального закона «О персональных данных».

4. Для проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах операторами и (или) уполномоченными лицами в соответствии с законодательством Российской Федерации могут привлекаться организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

5. Для обеспечения безопасности персональных данных при их обработке в информационных системах применяются средства защиты информации, прошедшие в соответствии с законодательством Российской Федерации оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации.

6. Оценка достаточности выбранных и реализованных в системе защиты персональных данных организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах для нейтрализации актуальных угроз безопасности персональных данных осуществляется оператором (уполномоченным лицом) в ходе проводимого им контроля за выполнением требований к защите персональных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119.

По решению оператора (уполномоченного лица) оценка достаточности выбранных и реализованных в системе защиты персональных данных организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах может осуществляться в рамках аттестации информационной системы.

7. Меры по обеспечению безопасности персональных данных в государственных информационных системах принимаются в соответствии с требованиями о защите информации, не содержащей государственную тайну, содержащейся в государственных информационных системах, устанавливаемыми ФСТЭК России в пределах своих полномочий.

II. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

8. В систему защиты персональных данных в зависимости от актуальных угроз безопасности персональных данных и структурно-функциональных характеристик информационной системы персональных данных включаются следующие меры:

– обеспечение доверенной загрузки;

– идентификацию и аутентификацию субъектов доступа и объектов доступа;

– управление доступом субъектов доступа к объектам доступа;

– ограничение программной среды;

– защиту машинных носителей информации;

– регистрацию событий безопасности;

– обеспечение целостности информационной системы и информации;

– защиту среды виртуализации;

– защиту технических средств;

– защиту информационной системы, ее средств и систем связи и передачи данных.

8.1. Меры по обеспечению доверенной загрузки должны исключать несанкционированное использование средств вычислительной техники и получение возможности доступа к персональным данным в обход системы защиты персональных данных.

Меры по обеспечению доверенной загрузки включают

– блокировку доступа к ресурсам средств вычислительной техники;

– блокировку загрузки нештатной операционной системы или программного обеспечения, способного модифицировать загрузочную область штатной операционной системы, в том числе со съемных машинных носителей информации;

– блокировку интерфейсов и цепей питания средств вычислительной техники.

8.2. Меры по идентификации и аутентификации должны обеспечивать присвоение субъектам доступа и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности).

Меры по идентификации и аутентификации включают

– идентификацию и аутентификацию пользователей, процессов, иных субъектов доступа;

– идентификацию и аутентификацию устройств (в том числе стационарных, мобильных и портативных), объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным программным обеспечением, иных объектов доступа;

– управление идентификаторами;

– управление средствами аутентификации;

– защиту обратной связи при вводе аутентификационной информации;

– идентификацию и аутентификацию внешних пользователей.

8.3. Меры по управлению доступом должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

Меры по управлению доступом включают

– управление учетными записями пользователей;

– управление предоставлением доступа субъектов доступа к объектам доступа (реализацию различных методов, типов и правил разграничения доступа), в том числе при совместном использовании информации несколькими субъектами доступа;

– управление информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;

– разделение обязанностей различных категорий пользователей и администраторов информационной системы;

– назначение минимальных прав и привилегий субъектам доступа;

– управление неуспешными попытками входа в информационную систему (доступа к информационной системе);

– оповещение пользователя о доступе к информационной системе, в которой реализованы меры защиты информации, при его входе в информационную систему;

– оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему;

– ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы;

– блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу;

– установление действий пользователей, разрешенных до идентификации и аутентификации;

– поддержку и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения, обработки и передачи;

– управление удаленным доступом субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;

– ограничение и контроль использования в информационной системе технологий беспроводного доступа;

– ограничение и контроль использования в информационной системе мобильных технических средств (устройств, машинных носителей информации);

– управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).

8.4. Меры по ограничению программной среды должны исключать установку (инсталляцию) неиспользуемого в обработке персональных данных или запрещенного к использованию программного обеспечения (в том числе средств разработки и отладки программ), а также их загрузку (запуск) после установки.

Меры по ограничению программной среды включают

– управление запуском (обращениями) компонентов программного обеспечения;

– управление установкой (инсталляцией) компонентов программного обеспечения;

– запрет установки (инсталляции) запрещенного к использованию программного обеспечения и (или) его компонентов, в том числе средств разработки и отладки;

– управление записью временных файлов.

8.5. Меры по защите машинных носителей информации должны исключать несанкционированный доступ к носителям и персональным данным, хранящимся на них, а также несанкционированное использование съемных машинных носителей информации.

Меры по защите машинных носителей информации включают

– маркировку и учет машинных носителей информации;

– управление доступом к машинным носителям информации;

– контроль перемещения машинных носителей информации за пределы контролируемой зоны;

– использование способов хранения персональных данных на машинных носителях информации, не позволяющих несанкционированно

ознакомиться с ее содержанием, а также использовать носитель информации в иных информационных системах;

- контроль использования интерфейсов ввода (вывода);
- контроль ввода (вывода) персональных данных на машинные носители информации;
- контроль подключения машинных носителей информации;
- уничтожение (стирание) персональных данных на машинных носителях информации;
- контроль уничтожения (стирания) персональных данных на машинных носителях информации.

8.6. Меры по регистрации событий безопасности должны обеспечивать распознавание, запись, хранение и защиту информации о событиях в информационной системе, относящихся к безопасности персональных данных, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

Меры по регистрации событий безопасности включают

- определение событий, относящихся к безопасности персональных данных и подлежащих регистрации;
- определение состава и содержания информации о событиях, относящихся к безопасности персональных данных и подлежащих регистрации;
- обеспечение возможности просмотра и анализа информации о действиях пользователей;
- резервирование необходимого объема памяти для записи информации о событиях, относящихся к безопасности персональных данных;
- запись (регистрация) информации о событиях, относящихся к безопасности персональных данных;
- реагирование на сбои при регистрации событий, относящихся к безопасности персональных данных, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения емкости памяти;
- просмотр и анализ результатов регистрации событий, относящихся к безопасности персональных данных, и реагирование на них;
- сокращение объема информации о событиях, относящихся к безопасности персональных данных, предоставляемой для просмотра и анализа;

- генерирование временных меток и синхронизация системного времени в информационной системе;
- защиту информации о событиях, относящихся к безопасности персональных данных;
- обеспечение необходимого времени хранения информации о событиях, относящихся к безопасности персональных данных.

8.7. Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов нарушения целостности информационной системы и информации, возможность восстановления информационной системы и информации, а также антивирусную защиту, обнаружение вторжений в информационную систему и реагирование на них.

Меры по обеспечению целостности информационной системы и персональных данных включают

- выявление, анализ и устранение уязвимостей и иных недостатков в программном обеспечении;
- контроль установки обновлений программного обеспечения;
- антивирусную защиту;
- обнаружение вторжений;
- контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;
- контроль целостности персональных данных и программного обеспечения;
- контроль состава технических средств обработки персональных данных и программного обеспечения;
- обеспечение возможности восстановления персональных данных и программного обеспечения;
- обнаружение и реагирование на факты передачи в информационную систему информации (сообщений), не относящейся к функционированию информационной системы (незапрашиваемых сообщений);
- ограничение прав пользователей по вводу информации в информационную систему;
- контроль точности, полноты и правильности информации, вводимой в информационную систему;

– контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных;

– прогнозирование и предотвращение возможных отказов технических средств, реагирование на отказы технических средств.

8.8. Меры по защите среды виртуализации должны исключать несанкционированный доступ к объектам защиты виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, гипервизору, системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

Меры по защите среды виртуализации включают

– аутентификацию компонентов виртуальной инфраструктуры, администраторов управления средствами виртуализации, терминальных устройств виртуальной инфраструктуры;

– управление доступом к компонентам виртуальной инфраструктуры;

– управление потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры;

– доверенную загрузку серверов виртуализации, виртуальной машины (контейнера) и серверов управления виртуализацией;

– разграничение доступа к данным, обрабатываемым в виртуальных машинах (контейнерах), и (или) изоляцию виртуальных машин (контейнеров);

– управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных;

– регистрацию событий в виртуальной инфраструктуре, относящихся к безопасности персональных данных;

– контроль целостности конфигураций компонентов виртуальной инфраструктуры и самих компонентов;

– резервное копирование данных, резервирование технических средств и (или) программного обеспечения виртуальной инфраструктуры, а также каналов связи виртуальной инфраструктуры;

– распределенное хранение данных и восстановление информации после сбоев;

– реализацию и управление антивирусной защитой и обнаружение вторжений, направленных на виртуальную инфраструктуру.

8.9. Меры по защите технических средств информационной системы должны обеспечивать ограничение доступа к техническим средствам обработки персональных данных, средствам обеспечения функционирования информационной системы и в помещения в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

Меры по защите технических средств включают

– защиту персональных данных от утечки по техническим каналам;

– защиту от несанкционированного физического доступа к средствам обработки персональных данных, средствам защиты информации и средствам обеспечения функционирования информационной системы;

– защиту от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов).

8.10. Меры по защите информационной системы, ее средств и систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии сегментов информационной системы, информационной системы с иными информационными системами и информационно-телекоммуникационными сетями.

Меры по защите информационной системы, ее средств и систем связи и передачи данных включают

– отделение (физическое, логическое) функциональных возможностей по управлению (администрированию) информационной системы и (или) ее сегментов, устройств от функциональных возможностей пользователей по использованию информационной системы;

– изоляцию (физическую, логическую) функций информационной системы, связанных с обеспечением безопасности персональных данных (функций безопасности), от иных функций информационной системы, не связанных с обеспечением безопасности персональных данных;

– исключение доступа текущего субъекта доступа к информации, полученной в результате действий предыдущего субъекта доступа, через общие ресурсы информационной системы (реестры, оперативную память, внешние запоминающие устройства и иные ресурсы);

– защиту информационной системы от действий нарушителей, приводящих к затруднению или невозможности доступа пользователей

к ресурсам этой информационной системы (защита от отказа в обслуживании);

- предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом;
- обеспечение защиты периметра информационной системы и периметров ее сегментов при взаимодействии информационной системы с иными информационными системами и информационно-телекоммуникационными сетями, а также при взаимодействии сегментов информационной системы, включая контроль потоков информации и управление потоками информации;
- обеспечение безопасности персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при их передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны;
- прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения;
- обеспечение доверенного взаимодействия (канала передачи данных) между пользователем и средствами защиты информации (функциями безопасности средств защиты информации);
- обеспечение целостности и доступности общедоступных персональных данных и программного обеспечения, предназначенного для их обработки (доступа к ним);
- запрет несанкционированной удаленной активации, включая физическое отключение, периферийных устройств (видеокамер, микрофонов и иных устройств, которые могут активироваться удаленно) и оповещение пользователей об активации таких устройств;
- передачу и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене персональными данными с иными информационными системами;
- контроль использования и исключение несанкционированного использования технологий мобильного кода, регистрацию событий, связанных с использованием технологии мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологии мобильного кода;
- контроль использования и исключение несанкционированного использования технологий передачи речи, регистрацию событий, связанных с использованием технологий передачи речи, их анализ и

реагирование на нарушения, связанные с использованием технологий передачи речи;

- контроль (подтверждение происхождения) источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам, обеспечение ее доступности и целостности;
- обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов;
- перевод (обеспечение возврата) информационной системы или ее устройств (компонентов) в заранее определенное состояние, обеспечивающее защиту персональных данных в случае возникновения отказов (сбоев) в системе защиты информации информационной системы;
- использование устройств, имеющих минимальные функциональные возможности и память для обработки и хранения персональных данных;
- создание (эмуляцию) несуществующих (ложных) информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей по реализации угроз безопасности персональных данных;
- использование при создании информационной системы различных типов общесистемного, прикладного и специального программного обеспечения;
- использование прикладного и специального программного обеспечения, функционирующего на различных типах операционных систем;
- обеспечение защиты информации (данных), которая не подлежит изменению в процессе функционирования информационной системы (архивные файлы, параметры настройки средств защиты информации и программного обеспечения и иная информация пользователей и информационной системы);
- воспроизведение несуществующих (ложных) и (или) сокрытие отдельных структурно-функциональных характеристик информационной системы и (или) параметров настройки средств защиты информации и программного обеспечения для введения в заблуждение нарушителей при реализации ими угроз безопасности персональных данных;
- выявление, анализ и блокирование при создании информационной системы скрытых каналов передачи информации в обход

реализованных мер по обеспечению безопасности персональных данных или внутри разрешенных сетевых протоколов;

– разбиение информационной системы на сегменты с учетом значимости обрабатываемых в них персональных данных и обеспечение защиты периметров сегментов информационной системы (сегментирование информационной системы);

– обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения.

– изоляция процессов (выполнение программ) в выделенной области памяти;

– защита внутренних и внешних беспроводных соединений, применяемых в информационной системе.

9. Блокирование (нейтрализация) актуальных угроз безопасности персональных данных обеспечивается посредством выбора и реализации в системе защиты персональных данных мер по обеспечению безопасности персональных данных.

Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в системе защиты персональных данных, включает

– выбор базового набора мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных, обрабатываемых в информационной системе, в соответствии с базовыми наборами мер по обеспечению безопасности персональных данных, приведенными в приложении к настоящему документу;

– адаптацию выбранного базового набора мер по обеспечению безопасности персональных данных применительно к структурно-функциональным характеристикам информационной системы, реализуемым информационным технологиям, особенностям функционирования информационной системы, а также с учетом целей защиты персональных данных (конфиденциальности, целостности, доступности);

– дополнение адаптированного базового набора мер по обеспечению безопасности персональных данных дополнительными мерами по обеспечению безопасности персональных данных, приведенными в приложении к настоящему документу, но не определенными в качестве базовых, и определение их содержания для обеспечения блокирования (нейтрализации) актуальных угроз безопасности персональных данных, а также дополнительными мерами, обеспечивающими выполнение требований по обеспечению безопасности персональных данных,

установленными иными нормативными правовыми актами в области защиты информации.

10. При невозможности и (или) нецелесообразности реализации в системе защиты персональных данных отдельных выбранных мер по обеспечению безопасности персональных данных взамен них могут применяться иные (компенсирующие) меры по обеспечению безопасности персональных данных, обеспечивающие нейтрализацию актуальных угроз безопасности персональных данных.

В этом случае в ходе проектирования системы защиты персональных данных должно быть проведено обоснование применения компенсирующих мер по обеспечению безопасности персональных данных для нейтрализации актуальных угроз безопасности персональных данных.

11. Меры по обеспечению безопасности персональных данных выбираются и реализуются в системе защиты персональных данных применительно ко всем объектам и субъектам доступа на аппаратном, системном, прикладном и сетевом уровнях, а также в среде виртуализации и облачных технологий.

12. Для обеспечения 4 уровня защищенности персональных данных в информационных системах персональных данных должны применяться средства защиты информации 6 класса защиты (6 класса защищенности средств вычислительной техники).

Для обеспечения 3 уровня защищенности персональных данных в информационных системах, в которых не определены в качестве актуальных угрозы 2-го типа и которые не подключены к информационно-телекоммуникационным сетям международного информационного обмена, должны применяться средства защиты информации не ниже 5 класса защиты (5 класса защищенности средств вычислительной техники).

Для обеспечения 1 и 2 уровня защищенности персональных данных в информационных системах персональных данных, а также 3 уровня защищенности персональных данных в информационных системах, в которых определены в качестве актуальных угрозы 2-го типа или которые подключены к информационно-телекоммуникационным сетям международного информационного обмена, должны применяться средства защиты информации не ниже 4 класса защиты (5 класса защищенности средств вычислительной техники).

13. При использовании в информационных системах новых информационных технологий и выявлении дополнительных угроз безопасности персональных данных, для которых в настоящем документе не определены меры по обеспечению безопасности персональных данных, должны разрабатываться компенсирующие меры в соответствии с пунктом 10 настоящего документа.

П р и л о ж е н и е к «Составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"

Базовый состав мер по обеспечению безопасности персональных данных для соответствующего уровня защищенности персональных данных, обрабатываемых в информационной системе

Номер и условное обозначение меры	Меры по обеспечению безопасности персональных данных	Уровень защищенности персональных данных			
		4	3	2	1
Обеспечение доверенной загрузки (ДЗГ)					
ДЗГ.1	Блокировка доступа к ресурсам средств вычислительной техники				+
ДЗГ.2	Блокировка загрузки нештатной операционной системы или программного обеспечения, способного модифицировать загрузочную область штатной операционной системы, в том числе со съемных машинных носителей информации				
ДЗГ.3	Блокировка интерфейсов и цепей питания средств вычислительной техники				
Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, процессов, иных субъектов доступа	+	+	+	+
ИАФ.2	Идентификация и аутентификация устройств (в том числе стационарных, мобильных и портативных), объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным программным обеспечением, иных объектов доступа			+	+
ИАФ.3	Управление идентификаторами	+	+	+	+
ИАФ.4	Управление средствами аутентификации	+	+	+	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+
ИАФ.6	Идентификация и аутентификация внешних пользователей	+	+	+	+
Управление доступом субъектов доступа к объектам доступа (УПД)					
УПД.1	Управление учетными записями пользователей	+	+	+	+

УПД.2	Управление предоставлением доступа субъектов доступа к объектам доступа (реализацию различных методов, типов и правил разграничения доступа), в том числе при совместном использовании информации несколькими субъектами доступа	+	+	+	+
УПД.3	Управление информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами			+	+
УПД.4	Разделение обязанностей различных категорий пользователей и администраторов информационной системы		+	+	+
УПД.5	Назначение минимальных прав и привилегий субъектам доступа		+	+	+
УПД.6	Управление неуспешными попытками входа в информационную систему (доступа к информационной системе)	+	+	+	+
УПД.7	Оповещение пользователя о доступе к информационной системе, в которой реализованы меры защиты информации, при его входе в информационную систему				+
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему				
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы				+
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		+	+	+
УПД.11	Установление действий пользователей, разрешенных до идентификации и аутентификации	+	+	+	+
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения, обработки и передачи				
УПД.13	Управление удаленным доступом субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+	+	+	+
УПД.14	Ограничение и контроль использования в информационной системе технологий беспроводного доступа	+	+	+	+

УПД.15	Ограничение и контроль использования в информационной системе мобильных технических средств (устройств, машинных носителей информации)	+	+	+	+
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	+	+	+
Ограничение программной среды (ОПС)					
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения				+
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения			+	+
ОПС.3	Запрет установки (инсталляции) запрещенного к использованию программного обеспечения и(или) его компонентов, в том числе средств разработки и отладки	+	+	+	+
ОПС.4	Управление записью временных файлов				
Защита машинных носителей информации (ЗНИ)					
ЗНИ.1	Маркировка и учет машинных носителей информации	+	+	+	+
ЗНИ.2	Управление доступом к машинным носителям информации	+	+	+	+
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны				
ЗНИ.4	Использование способов хранения информации на машинных носителях информации, не позволяющих несанкционированно ознакомиться с ее содержанием, а также использовать носитель информации в иных информационных системах				
ЗНИ.5	Контроль использования интерфейсов ввода (вывода)			+	+
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации				
ЗНИ.7	Контроль подключения машинных носителей информации				
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях	+	+	+	+
ЗНИ.9	Контроль уничтожения (стирания) информации на машинных носителях	+	+	+	+

Регистрация событий безопасности (РСБ)					
РСБ.1	Определение событий, относящихся к безопасности персональных данных, и подлежащих регистрации	+	+	+	+
РСБ.2	Определение состава и содержания информации о событиях, относящихся к безопасности персональных данных, и подлежащих регистрации	+	+	+	+
РСБ.3	Обеспечение возможности просмотра и анализа информации о действиях пользователей				
РСБ.4	Резервирование необходимого объема памяти для записи информации о событиях, относящихся к безопасности персональных данных	+	+	+	+
РСБ.5	Запись (регистрация) информации о событиях, относящихся к безопасности персональных данных	+	+	+	+
РСБ.6	Реагирование на сбои при регистрации событий, относящихся к безопасности персональных данных, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения емкости памяти	+	+	+	+
РСБ.7	Просмотр и анализ результатов регистрации событий, относящихся к безопасности персональных данных, и реагирование на них	+	+	+	+
РСБ.8	Сокращение объема информации о событиях, относящихся к безопасности персональных данных, предоставляемой для просмотра и анализа			+	+
РСБ.9	Генерирование временных меток и синхронизация системного времени в информационной системе	+	+	+	+
РСБ.10	Защита информации о событиях, относящихся к безопасности персональных данных	+	+	+	+
РСБ.11	Обеспечение необходимого времени хранения информации о событиях, относящихся к безопасности персональных данных	+	+	+	+
Обеспечение целостности информационной системы и информации (ОЦЛ)					
ОЦЛ.1	Выявление, анализ и устранение уязвимостей и иных недостатков в программном обеспечении	+	+	+	+

ОЦЛ.2	Контроль установки обновлений программного обеспечения	+	+	+	+
ОЦЛ.3	Антивирусная защита	+	+	+	+
ОЦЛ.4	Обнаружение вторжений			+	+
ОЦЛ.5	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации			+	+
ОЦЛ.6	Контроль целостности информации и программного обеспечения			+	+
ОЦЛ.7	Контроль состава технических средств обработки информации и программного обеспечения	+	+	+	+
ОЦЛ.8	Обеспечение возможности восстановления информации и программного обеспечения	+	+	+	+
ОЦЛ.9	Обнаружения и реагирование на факты передачи в информационную систему информации (сообщений), не относящиеся к функционированию информационной системы (незапрашиваемых сообщений)			+	+
ОЦЛ.10	Ограничение прав пользователей по вводу информации в информационную систему			+	+
ОЦЛ.11	Контроль точности, полноты и правильности информации, вводимой в информационную систему				
ОЦЛ.12	Контроль ошибочных действий пользователей по вводу и (или) передаче информации конфиденциального характера				
ОЦЛ.13	Прогнозирование и предотвращение возможных отказов технических средств, реагирование на отказы технических средств				
Защита среды виртуализации (ЗСВ)					
ЗСВ.1	Аутентификация компонентов виртуальной инфраструктуры, администраторов управления средствами виртуализации, терминальных устройств виртуальной инфраструктуры			+	+
ЗСВ.2	Управление доступом к компонентам виртуальной инфраструктуры	+	+	+	+
ЗСВ.3	Управление потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры			+	+
ЗСВ.4	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера) и серверов управления виртуализацией				

ЗСВ.5	Разграничение доступа к данным, обрабатываемым в виртуальных машинах (контейнерах), и (или) изоляция виртуальных машин (контейнеров)			+	+
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных			+	+
ЗСВ.7	Регистрация событий в виртуальной инфраструктуре, относящихся к безопасности персональных данных	+	+	+	+
ЗСВ.8	Контроль целостности конфигураций компонентов виртуальной инфраструктуры и самих компонентов			+	+
ЗСВ.9	Резервное копирование данных, резервирование технических средств и (или) программного обеспечения виртуальной инфраструктуры, а также каналов связи виртуальной инфраструктуры		+	+	+
ЗСВ.10	Распределенное хранение данных и восстановление информации после сбоев				+
ЗСВ.11	Реализация и управление антивирусной защитой и обнаружение вторжений, направленных на виртуальную инфраструктуру			+	+
Защита технических средств (ЗТС)					
ЗТС.1	Защита информации от ее утечки по техническим каналам				
ЗТС.2	Защита от несанкционированного физического доступа к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы	+	+	+	+
ЗТС.3	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)				
Защита информационной системы, ее средств и систем связи и передачи данных (ЗИС)					
ЗИС.1	Отделение (физическое, логическое) функциональных возможностей по управлению (администрированию) информационной системы и (или) ее сегментов, устройств от функциональных возможностей пользователей по использованию информационной системы			+	+

ЗИС.2	Изоляция (физическая, логическая) функций информационной системы, связанных с обеспечением защиты информации (функций безопасности), от иных функций информационной системы, не связанных с обеспечением безопасности персонал.данных				+
ЗИС.3	Исключение доступа текущего субъекта доступа к информации, полученной в результате действий предыдущего субъекта доступа, через общие ресурсы информационной системы (реестры, оперативную память, внешние запоминающие устройства и иные ресурсы)				+
ЗИС.4	Защита информационной системы от действий нарушителей, приводящих к затруднению или невозможности доступа пользователей к ресурсам этой информационной системы (защита от отказа в обслуживании)		+	+	+
ЗИС.5	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				+
ЗИС.6	Обеспечение защиты периметра информационной системы и периметров ее сегментов при взаимодействии информационной системы с иными информационными системами и информационно-телекоммуникационными сетями, а также при взаимодействии сегментов информационной системы, включая контроль потоков информации и управление потоками информации	+	+	+	+
ЗИС.7	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при их передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны	+	+	+	+
ЗИС.8	Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения			+	+
ЗИС.9	Обеспечение доверенного взаимодействия (канала передачи данных) между пользователем и средствами защиты информации (функциями безопасности средств защиты информации)				

ЗИС.10	Обеспечение целостности и доступности общедоступных персональных данных и программного обеспечения, предназначенного для их обработки (доступа к ним)	+	+	+	+
ЗИС.11	Запрет несанкционированной удаленной активации, включая физическое отключение, периферийных устройств (видеокамер, микрофонов и иных устройств, которые могут активироваться удаленно) и оповещение пользователей об активации таких устройств	+	+	+	+
ЗИС.12	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационными системами				
ЗИС.13	Контроль использования и исключение несанкционированного использования технологий мобильного кода, регистрация событий, связанных с использованием технологии мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологии мобильного кода			+	+
ЗИС.14	Контроль использования и исключение несанкционированного использования технологий передачи речи, регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи			+	+
ЗИС.15	Контроль (подтверждение происхождения) источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам, обеспечение ее доступности и целостности	+	+	+	+
ЗИС.16	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов			+	+
ЗИС.17	Перевод (обеспечение возврата) информационной системы или ее устройств (компонентов) в заранее определенное состояние, обеспечивающее защиту персональных данных в случае возникновения отказов (сбоев) в системе защиты информации информационной системы				+

ЗИС.18	Использование устройств, имеющих минимальные функциональные возможности и память для обработки и хранения персональных данных				
ЗИС.19	Создание (эмуляция) несуществующих (ложных) информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей по реализации угроз безопасности информации				
ЗИС.20	Использование при создании информационной системы различных типов общесистемного, прикладного и специального программного обеспечения				
ЗИС.21	Использование прикладного и специального программного обеспечения, функционирующего на различных типах операционных систем				
ЗИС.22	Обеспечение защиты информации (данных), которая не подлежит изменению в процессе функционирования информационной системы (архивные файлы, параметры настройки средств защиты информации и программного обеспечения и иная информация пользователей и информационной системы)			+	+
ЗИС.23	Воспроизведение несуществующих (ложных) и (или) скрытие отдельных структурно-функциональных характеристик информационной системы и (или) параметров настройки средств защиты информации и программного обеспечения для введения в заблуждение нарушителей при реализации ими угроз безопасности персональных данных				
ЗИС.24	Выявление, анализ и блокирование при создании информационной системы скрытых каналов передачи информации в обход реализованных мер по обеспечению безопасности персональных данных или внутри разрешенных сетевых протоколов				
ЗИС.25	Разбиение информационной системы на сегменты с учетом значимости обрабатываемой в них персональных данных и обеспечение защиты периметров сегментов информационной системы (сегментирование информационной системы)			+	+

ЗИС.26	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения				
ЗИС.27	Изоляция процессов (выполнение программ) в выделенной области памяти				
ЗИС.28	Защита внутренних и внешних беспроводных соединений, применяемых в информационной системе	+	+	+	+

Примечание

«+» — мера по обеспечению безопасности персональных данных применяется в качестве базовой для обеспечения безопасности персональных соответствующего уровня защищенности персональных данных.

Меры по обеспечению безопасности персональных данных, не обозначенные знаком «+», применяются при адаптации базового набора мер, дополнения адаптированного базового набора мер, а также при разработке компенсирующих мер по обеспечению безопасности персональных данных соответствующего уровня защищенности.

В 2009 г. университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена Программа развития государственного образовательного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет информационных технологий, механики и оптики» на 2009–2018 г.г.

КАФЕДРА УПРАВЛЕНИЯ ГОСУДАРСТВЕННЫМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

Кафедра УГИС создана в 2011 г. на магистерском корпоративном факультете НИУ ИТМО.

Обучение по магистерской программе «Управление государственными информационными системами» направлено на приобретение теоретических знаний и практических навыков в сфере создания и развития ИТ-систем для нужд государственной власти и местного самоуправления.

Практическая часть обучения проходит на базе Центра технологий электронного правительства НИУ ИТМО, Санкт-Петербургского информационно-аналитического центра и других партнерских структур под руководством опытных экспертов и представителей органов власти.

М. И. Шубинский

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЛЯ РАБОТНИКОВ БЮДЖЕТНОЙ СФЕРЫ. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Учебное пособие

В авторской редакции
Дизайн С.Н. Ушаков
Вёрстка Е.Е. Нестерова
Корректор Т.А. Асанович
Редакционно-издательский отдел Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики
Зав. РИО Н. Ф. Гусарова
Лицензия ИД № 00408 от 05.11.99
Подписано к печати
Заказ №
Тираж 50 экз.
Отпечатано на ризографе