МЕтодические рекомендации

ПО ОБЕСПЕЧЕНИЮ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ МЕДИЦИНСКИХ ОРГАНИЗАЦИЙ

Белгород 2015

**АННОТАЦИЯ**

Документ предназначен для использования специалистами по обеспечению безопасности информации в учреждениях здравоохранения Белгородской области, руководителей учреждений здравоохранения Белгородской области, организующих и проводящих работы по обработке персональных данных (далее – ПДн) в информационных системах персональных данных (далее – ИСПДн).

**СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ**

| Сокращение | Определение |
| --- | --- |
| БД | База данных |
| ПДн | Персональные данные |
| ИСПДн | Информационная система персональных данных |
| ИС | Информационная система |
| НСД | Несанкционированный доступ |
| ОМС | Обязательное медицинское страхование |
| ДМС | Добровольное медицинское страхование |
| ФСТЭК | Федеральная служба технического и экспортного контроля |
| СЗИ | Средства защиты информации |
| СКЗИ | Средства криптографической защиты информации |
| СВТ | Средства вычислительной техники |
| ПО | Программное обеспечение |
| СА | Системный администратор |
| АБ | Администратор безопасности |

# РЕКОМЕНДАЦИИ ПО ОПРЕДЕЛЕНИЮ УРОВНЯ ЗАЩИЩЕННОСТИ ИСПДн УЧРЕЖДЕНИЙ

Определение уровня защищенности ИСПДн производится на основании постановления правительства Российской Федерации № 1119 от 01.11.2012 года «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Для определения уровня защищенности ИСПДн необходимо:

* + 1. ***Определить тип ИСПДн.***

Существует 4 типа ИСПДн: 1. Обрабатывающая специальные категории персональных данных (ИСПДн-С), 2. Обрабатывающая биометрические персональные данные (ИСПДн-Б) 3. Обрабатывающая общедоступные персональные данные (ИСПДн-О) 4. Обрабатывающая иные категории персональных данных (ИСПДн-И).

1. Информационная система является информационной системой, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.
2. Информационная система является информационной системой, обрабатывающей биометрические персональные данные, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.
3. Информационная система является информационной системой, обрабатывающей общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона «О персональных данных».
4. Информационная система является информационной системой, обрабатывающей иные категории персональных данных, если в ней не обрабатываются персональные данные, указанные в абзацах первом - третьем настоящего пункта.
   * 1. ***Определить обрабатываются ли персональные данные сотрудников оператора (Да/Нет).***
     2. ***Определить количество субъектов, обрабатываемых в ИСПДн (более чем 100 000/менее чем 100 000).***
     3. ***Определить тип актуальности угроз.***

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

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

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

В результате в соответствии с Таблицей 1 определить уровень защищенности необходимо для каждой ИСПДн.

Таблица 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Тип ИСПДн** | **Сотрудники оператора** | **Количество субъектов** | **Тип актуальных угроз** | | |
| **1** | **2** | **3** |
| ИСПДн-С | Нет | >100 000 | УЗ-1 | УЗ-1 | УЗ-2 |
| Нет | < 100 000 | УЗ-1 | УЗ-2 | УЗ-3 |
| Да | Любое |
| ИСПДн-Б | Не важно | Любое | УЗ-1 | УЗ-2 | УЗ-3 |
| ИСПДн-И | Нет | >100 000 | УЗ-1 | УЗ-2 | УЗ-3 |
| Нет | < 100 000 | УЗ-1 | УЗ-3 | УЗ-4 |
| Да | Любое |
| ИСПДн-О | Нет | >100 000 | УЗ-2 | УЗ-2 | УЗ-4 |
| Нет | < 100 000 | УЗ-2 | УЗ-3 | УЗ-4 |
| Да | Любое |

Уровень защищенности оформляется актом. Для определения уровня защищенности приказом назначается комиссия.

# СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

При обработке персональных данных необходимо организовать получение, учет и хранение письменного согласия субъектов ПДн (пациентов, сотрудников учреждения) на обработку их ПДн в необходимых случаях (статьи 6, 9, 10 закона № 152-ФЗ, часть 3 статьи 13 закона № 323-ФЗ). Состав реквизитов сведений, указываемых в согласии, перечислен в статье 9. Отметим, что оформление письменного согласия медицинского работника на обработку его ПДн в учреждении не требуется. Также теперь не требуется и согласие на передачу его ПДн в федеральный регистр медицинских и фармацевтических работников, поскольку это предусмотрено статьями 92 и 93 закона № 323-ФЗ. Необходимость оформления письменного согласия работника возникает в том случае, если в базе данных ИС учреждения хранится его фотография и (или) она публикуется на сайте в сети Интернет, что в последнее время достаточно часто практикуется (согласие на это может быть включено в текст трудового договора с работником). Фотография («изображение лица») относится к так называемым биометрическим данным, на основании которых можно установить личность человека, и обработка которых, в том числе публикация, может осуществляться только на основании письменного согласия субъекта персональных данных (статья 11 закона № 152-ФЗ).

Письменное согласие пациента не требуется в случаях, если: (а) медицинская помощь оказывается по программе ОМС и персональные данные, в том числе содержащие сведения, составляющие врачебную тайну (о состоянии здоровья), передаются только в территориальный фонд ОМС и страховую медицинскую организацию, что предусмотрено статьями 34, 38, 39, 43, 44 и 48 закона № 326-ФЗ; (б) персональные данные пациента, составляющие врачебную тайну, передаются третьим лицам, когда (часть 4 статьи 13 закона № 323-ФЗ):

1) это необходимо по экстренным показаниям и пациент в результате своего состояния не способен выразить свою волю;

2) при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

3) по запросу органов дознания и следствия, суда, органа уголовно-исполнительной системы;

4) в случае оказания медицинской помощи не совершеннолетнему для информирования одного из его родителей или иного законного представителя;

5) в целях информирования органов внутренних дело поступлении пациента, в отношении которого имеются основания полагать, что вред его здоровью причинен в результате противоправных действий (см. также п. 9 части 1 статьи 79 закона № 323-ФЗ, где говорится об обязанности медицинских организаций информировать органы внутренних дел в указанных случаях);

6) в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов и военно-врачебных (врачебно-летных) комиссий;

7) в целях расследования несчастного случая на производстве и профессионального заболевания;

8) при обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи (следует заметить, что определение понятия «медицинская информационная система» в законе № 323-ФЗ отсутствует);

9) в целях осуществления учета и контроля в системе обязательного социального страхования;

10) в целях осуществления контроля качества и безопасности медицинской деятельности в соответствии с законом № 323-ФЗ (см. статьи 87–90). Как видно, в новом законе № 323-ФЗ расширен перечень ситуаций, когда сведения, составляющие врачебную тайну, могут быть предоставлены без согласия пациента или его законного представителя.

Письменное согласие пациента на передачу (предоставление) его персональных данных, составляющих врачебную тайну, требуется в случаях, когда: (а) медицинская помощь оказывается за плату, вне программы государственных гарантий и сведения передаются третьим лицам (организациям), не являющимися медицинскими организациями, например, в страховую компанию и (или) страхователю по ДМС (в случае, если им не является сам пациент или его законный представитель); (б) информация о состоянии его здоровья передается лицам, указанным самим пациентом или его законным представителем (статья 19 закона № 323-ФЗ); в согласии должны быть указаны Ф.И.О. и контактные данные этих лиц (при этом можно считать, что пациент является представителем этих лиц, в связи с чем их специальное письменное согласие на обработку (хранение) указанных ПДн в медицинском учреждении не требуется (части 1 и 8 статьи 9 закона № 152-ФЗ); (в) передача персональных данных (документов) пациента осуществляется по открытым каналам связи (сети Интернет, электронной почте), например, при проведении дистанционных (телемедицинских) консультаций; (г) осуществляется трансграничная передача персональных данных пациента, например, при осуществлении телемедицинских консультаций с участием врачей, находящихся в странах, не являющихся сторонами Конвенции Совета Европы по защите физических лиц при автоматизированной обработке персональных данных или не включенных перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, утверждаемый Роскомнадзором (статья 12 закона № 152-ФЗ). Перечень этих стран можно посмотреть на сайте Роскомнадзора.

В случаях, когда в ИС медицинского учреждения хранятся и обрабатываются биометрические данные пациента (данные геометрии контура кисти руки, изображения отпечатка пальца, сосудистого русла, изображение радужной оболочки глаза, изображение (фотография) лица, данные ДНК и др.), также необходимо его специальное письменное согласие (статья 11 закона № 152-ФЗ).

В случаях, когда пациент отказывается предоставить свои персональные данные, сотрудник медицинского учреждения обязан разъяснить ему юридические последствия отказа (часть 2 статьи 18 закона № 152-ФЗ), в частности: (а) возможность получения медицинской помощи анонимно только за плату, за исключением случаев оказания ургентной помощи (статья 84 закона № 323-ФЗ); (б) практическую невозможность предъявления претензий по поводу качества лечения, в том числе в суд, поскольку процедурно сложной становится персонализация и аутентификация медицинской документации, оформленной на анонима – без документированной процедуры установления личности пациента (об этом пациент должен быть предупрежден во всех случаях анонимного обращения за медицинской помощью).

Следует обратить внимание, что хотя оформление письменного согласия пациента на обработку его персональных данных в лечебном учреждении, где он получает медицинскую помощь, в общем случае и не является теперь обязательным, в тоже время пациент имеет право обратиться в учреждение с заявлением о прекращении обработки его ПДн (часть 2 статьи 9 закона № 152-ФЗ). В случае отзыва согласия пациентом медицинское учреждение имеет право продолжить обработку его персональных данных (часть 2 статьи 9, часть 2 статьи 10, п. 7 части 1 статьи 6 новой редакции закона № 152-ФЗ), в частности, хранить и обрабатывать данные персонифицированного учета об оказанной пациенту медицинской помощи, необходимые для формирования и выставления счета на оплату по медицинскому страхованию (срок исковой давности – 3 года), записи в электронной медицинской карте пациента (срок хранения – 25 лет) и т.д. В прежней редакции закона при отзыве согласия во всех случаях оператор был обязан в течение трех дней прекратить обработку и уничтожить персональные данные. Отзыв согласия пациента на обработку его ПДн осуществляется в письменной форме. При этом, как уже было отмечено выше, субъект ПДн должен быть предупрежден о правовых последствиях прекращения дальнейшей автоматизированной обработки его персональных данных в медицинском учреждении.

1. **НОРМАТИВНО-ПРАВОВАЯ БАЗА ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

В настоящее время в области защиты персональных данных действуют следующие нормативные правовые акты:

1. Федеральный закон Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных».

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

4. «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утверждено Постановлением Правительства РФ от 15 сентября 2008 года № 687.

5. «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утверждены Постановлением Правительства РФ от 6 июля 2008 года № 512.

**Основные требования Федерального закона Российской Федерации «Об информации, информационных технологиях и о защите информации».**

П. 2 статьи 5 определяет, что информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

Обладателем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование (статья 6).

Ограничение доступа к информации устанавливается федеральными законами (статья 9).

Требования по защите информации для оператора ИС определены статьей 16, в которой сказано, что оператор ИС в случаях установленных законодательством обязан обеспечить:

- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

- своевременное обнаружение фактов несанкционированного доступа к информации;

- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

- постоянный контроль за обеспечением уровня защищенности информации.

Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации определены в статье 17. Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

**Основные требования Федерального закона Российской Федерации «О персональных данных».**

В статье 3 даны основные понятия, используемые в настоящем Федеральном законе:

- Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

- Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

- Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Обработка персональных данных осуществляется только с согласия субъекта персональных данных в случаях установленных законодательством (статья 6).

Законом введено понятие специальной категории персональных данных, т.е. данных о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни. Если иное не установлено другими федеральными законами, то обработка данной информации оператором не допускается (статья 10).

Статья 19 определяет, что оператор при обработке ПДн обязан принимать необходимые организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования… и иных неправомерных действий.

Ч. 2 статьи 19 определяет какими путями достигается обеспечение безопасности персональных данных.

Статья 22.1. определяет, что:

- Оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных.

- Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

1) осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2) доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

В соответствии с Федеральным Законом № 59, подписанным Президентом РФ 23 декабря 2010 года «О внесении изменений в статью 25 Федерального закона «О персональных данных» пункт 3 статьи 25 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» изложен в следующей редакции:

«Информационные системы персональных данных, созданные до 1 января 2011 года, должны быть приведены в соответствие с требованиями настоящего Федерального закона не позднее 1 июля 2011 года».

**Основные требования «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» утвержденное Постановлением Правительства РФ от 15 сентября 2008 года № 687 во исполнение требований ч. 3 ст. 19 Федерального закона «О персональных данных».**

В разделе I «Общие положения»:

Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее - персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации, должны применяться с учетом требований настоящего Положения.

В разделе II «Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации» определены требования:

- к носителям персональных данных;

- обязательность информирования сотрудников организации о факте обработке ими персональных данных, правилах обработки персональных данных;

- условия использования (ведения) в организации типовых форм, журналов, реестров, книг, в которые заносятся персональные данные;

- условия уничтожения или обезличивания персональных данных.

В разделе III «Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации»:

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

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

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

**Постановление Правительства РФ от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных и уровни защищенности таких данных.**

Данный документ определяет 4 уровня защищенности для информационных систем персональных данных и для каждого уровня защищенности необходимый набор требований:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Требования** | **Уровни защищенности** | | | |
| **1** | **2** | **3** | **4** |
| Режим обеспечения безопасности помещений, где обрабатываются персональные данных | + | + | + | + |
| Сохранность носителей персональных данные | + | + | + | + |
| Перечень лиц, допущенных к персональным данным | + | + | + | + |
| СЗИ, прошедшие процедуру оценки соответствия | + | + | + | + |
| Должностное лицо, ответственное за обеспечение безопасности персональных данных в ИСПДн | + | + | + | - |
| Ограничение доступа к содержанию электронного журнала сообщений | + | + | - | - |
| Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным | + | - | - | - |
| Структурное подразделение, ответственное за обеспечение безопасности персональных данных | + | - | - | - |

ФСТЭК России разработаны следующие документы, регламентирующие вопросы обеспечения безопасности ПДн в информационных системах.

1. Приказ ФСТЭК России № 21 от 18.02.2013 года «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

2. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена 15 февраля 2008 года заместителем директора ФСТЭК России.

3. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена 14 февраля 2008 года заместителем директора ФСТЭК России.

4. Приказ ФСТЭК России № 21 от 18.02.2013 года «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Приказ ФСТЭК № 21 от 18.02.2013 года устанавливает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для каждого из уровней защищенности персональных данных, установленных в Требованиях к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 года №1119.

В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

* идентификация и аутентификация субъектов доступа и объектов доступа;
* управление доступом субъектов доступа к объектам доступа;
* ограничение программной среды;
* защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);
* регистрация событий безопасности;
* антивирусная защита;
* обнаружение (предотвращение) вторжений;
* контроль (анализ) защищенности персональных данных;
* обеспечение целостности информационной системы и персональных данных;
* обеспечение доступности персональных данных;
* защита среды виртуализации;
* защита технических средств;
* защита информационной системы, ее средств, систем связи и передачи данных;
* выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
* управление конфигурацией информационной системы и системы защиты персональных данных.

Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены ниже в таблице:

| **Условное обозначение и номер меры** | **Содержание мер по обеспечению безопасности персональных данных** | **Уровни защищенности персональных данных** | | | |
| --- | --- | --- | --- | --- | --- |
| **4** | **3** | **2** | **1** |
| I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | | | | | |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора | + | + | + | + |
| ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных |  |  | + | + |
| ИАФ.З | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов | + | + | + | + |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации | + | + | + | + |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации | + | + | + | + |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) | + | + | + | + |
| II. Управление доступом субъектов доступа к объектам доступа (УПД) | | | | | |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей | + | + | + | + |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа | + | + | + | + |
| УПД.З | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами | + | + | + | + |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы | + | + | + | + |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы | + | + | + | + |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) | + | + | + | + |
| УПД.7 | Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных |  |  |  |  |
| 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 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации |  | + | + | + |
| УПД.12 | Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки |  |  |  |  |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети | + | + | + | + |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа | + | + | + | + |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств | + | + | + | + |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | + | + | + | + |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники |  |  | + | + |
| III. Ограничение программной среды (ОПС) | |  | | | |
| ОПС.1 | Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения |  |  |  |  |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения |  |  | + | + |
| ОПС.З | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов |  |  |  | + |
| ОПС.4 | Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов |  |  |  |  |
| IV. Защита машинных носителей персональных данных (ЗНИ) | | | | | |
| ЗНИ.1 | Учет машинных носителей персональных данных |  |  | + | + |
| ЗНИ. 2 | Управление доступом к машинным носителям персональных данных |  |  | + | + |
| ЗНИ.З | Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны |  |  |  |  |
| ЗНИ.4 | Исключение возможности несанкционированного ознакомления с содержанием персональных данных,хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах |  |  |  |  |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных |  |  |  |  |
| ЗНИ.6 | Контроль ввода (вывода) информации на машинные носители персональных данных |  |  |  |  |
| ЗНИ.7 | Контроль подключения машинных носителей персональных данных |  |  |  |  |
| ЗНИ.8 | Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания |  | + | + | + |
| V. Регистрация событий безопасности (РСБ) | |  | | | |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | + | + | + | + |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | + | + | + | + |
| РСБ.З | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения | + | + | + | + |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти |  |  |  |  |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них |  |  | + | + |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе |  |  |  |  |
| РСБ. 7 | Защита информации о событиях безопасности | + | + | + | + |
| VI. Антивирусная защита (АВЗ) | | | | | |
| АВ3.1 | Реализация антивирусной защиты | + | + | + | + |
| АВ3.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | + | + | + | + |
| VII. Обнаружение вторжений (СОВ) | | | | | |
| COB.l | Обнаружение вторжений |  |  | + | + |
| COB.2 | Обновление базы решающих правил |  |  | + | + |
| VIII. Контроль (анализ) защищенности персональных данных (АНЗ) | | | | | |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |  | + | + | + |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | + | + | + | + |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |  | + | + | + |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации |  | + | + | + |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе |  |  | + | + |
| IХ. Обеспечение целостности информационной системы и персональных данных (ОЦЛ) | | | | | |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации |  |  | + | + |
| ОЦЛ.2 | Контроль целостности персональных данных, содержащихся в базах данных информационной системы |  |  |  |  |
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций |  |  |  |  |
| ОЦЛ.4 | Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) |  |  | + | + |
| ОЦЛ. 5 | Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов),методов), и исключение неправомерной передачи информации из информационной системы |  |  |  |  |
| ОЦЛ.6 | Ограничение прав пользователей по вводу информации в информационную систему |  |  |  |  |
| ОЦЛ.7 | Контроль точности, полноты и правильности данных, вводимых в информационную систему |  |  |  |  |
| ОЦЛ.8 | Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях |  |  |  |  |
| X. Обеспечение доступности персональных данных (ОДТ) | | | | | |
| ОДТ.1 | Использование отказоустойчивых технических средств |  |  |  |  |
| ОДТ.2 | Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы |  |  |  |  |
| ОДТ.3 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |  |  |  | + |
| ОДТ.4 | Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных |  |  | + | + |
| ОДТ. 5 | Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала |  |  | + | + |
| XI. Защита среды виртуализации (ЗСВ) | | | | | |
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации | + | + | + | + |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин | + | + | + | + |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре |  | + | + | + |
| ЗСВ.4 | Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры |  |  |  |  |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |  |  |  |  |
| ЗСВ.6 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных |  |  | + | + |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигураций |  |  | + | + |
| ЗСВ. 8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры |  |  | + | + |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре |  | + | + | + |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей |  | + | + | + |
| XII. Защита технических средств (ЗТС) | | | | | |
| ЗТС.1 | Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам |  |  |  |  |
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования |  |  |  |  |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены | + | + | + | + |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | + | + | + | + |
| ЗТС.5 | Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) |  |  |  |  |
| XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС) | | | | | |
| ЗИС.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы |  |  |  | + |
| ЗИС.2 | Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом |  |  |  |  |
| ЗИС.3 | Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи | + | + | + | + |
| ЗИС.4 | Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) |  |  |  |  |
| ЗИС. 5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств |  |  |  |  |
| ЗИС.6 | Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами |  |  |  |  |
| ЗИС. 7 | Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода |  |  |  |  |
| ЗИС. 8 | Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи |  |  |  |  |
| ЗИС.9 | Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации |  |  |  |  |
| ЗИС.10 | Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам |  |  |  |  |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов |  |  | + | + |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю |  |  |  |  |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя |  |  |  |  |
| ЗИС.14 | Использование устройств терминального доступа для обработки персональных данных |  |  |  |  |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных |  |  | + | + |
| ЗИС.16 | Выявление, анализ и блокирование в информационной системы скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов |  |  |  |  |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы |  |  | + | + |
| ЗИС.18 | Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения |  |  |  |  |
| ЗИС.19 | Изоляция процессов (выполнение программ) в выделенной области памяти |  |  |  |  |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе |  | + | + | + |
| XIV. Выявление инцидентов и реагирование на них (ИНЦ) | | | | | |
| ИНЦ.1 | Определение лиц, ответственных за выявление инцидентов и реагирование на них |  |  | + | + |
| ИНЦ.2 | Обнаружение, идентификация и регистрация инцидентов |  |  | + | + |
| ИНЦ.3 | Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами |  |  | + | + |
| ИНЦ.4 | Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий |  |  | + | + |
| ИНЦ. 5 | Принятие мер по устранению последствий инцидентов |  |  | + | + |
| ИНЦ. 6 | Планирование и принятие мер по предотвращению повторного возникновения инцидентов |  |  | + | + |
| XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ) | | | | | |
| УКФ.1 | Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных |  | + | + | + |
| УКФ.2 | Управление изменениями конфигурации информационной системы и системы защиты персональных данных |  | + | + | + |
| УКФ.3 | Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных |  | + | + | + |
| УКФ.4 | Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных |  | + | + | + |

**Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.**

В «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» дается систематизированный перечень угроз безопасности информации, устанавливаются единые исходные данные по угрозам, определяются основные классы уязвимости, виды возможных деструктивных воздействий на информацию, а также основные способы их реализации.

Базовая модель угроз безопасности персональных данных содержит:

* Классификацию угроз безопасности персональных данных.
* Анализ и характеристики угроз возможной утечки по техническим каналам.
* Анализ и характеристики угроз несанкционированного доступа к информации в информационной системе персональных данных, включая характеристики источников угроз несанкционированного доступа, характеристики уязвимостей системного и прикладного программного обеспечения, характеристики угроз безопасности персональных данных, реализуемых с использованием протоколов межсетевого взаимодействия и программно-математических воздействий, характеристики нетрадиционных информационных каналов и результатов несанкционированного или случайного доступа.

Типовые модели угроз безопасности персональных данных, обрабатываемых в информационных системах (автоматизированных рабочих местах, локальных и распределенных информационных системах) не имеющих и имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

На основе базовой модели угроз должны разрабатываться частные модели угроз для конкретных систем персональных данных, учитывающие их особенности и многообразие. Для разработки этих частных моделей будет использоваться «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

**Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.**

Предназначена для формирования перечня актуальных угроз безопасности персональным данным, обрабатываемым в конкретной информационной системе, и разработке на его основе частной модели угроз для этой системы.

Формирование перечня источников угроз персональным данным осуществляется методом экспертного опроса. На основе экспертного опроса и анализа результатов сетевого сканирования информационной системы формируется перечень ее уязвимых звеньев. По данным обследования информационной системы формируется перечень возможных технических каналов утечки информации.

Путем анализа указанных перечней определяются условия существования в информационной системе угроз безопасности информации и составляется их полный перечень.

На основании полного перечня угроз безопасности информации в соответствии с порядком определения актуальных угроз безопасности персональных данных в информационных системах персональных данных формируется перечень актуальных угроз безопасности персональным данным в информационной системе.

Классификация угроз утечки информации по техническим каналам приведена ниже в таблице:

|  |  |
| --- | --- |
| **Угрозы утечки информации по техническим каналам** | **Каналы утечки** |
| Угрозы утечки акустической (речевой) информации | Акустические излучения информативного речевого сигнала |
| Виброакустические сигналы, возникающие посредством преобразования акустического сигнала при его воздействии на строительные конструкции и инженерно-технические коммуникации |
| Электрические сигналы, возникающие за счет акустоэлектрических преобразований |
| Радиоизлучения, модулированные информативным сигналом, возникающие за счет облучения технических средств ВЧ сигналом |
| Оптические излучения, за счет акустооптических преобразований (свойство волоконно-оптических линий) |
| Специальные электронные устройства съема речевой информации |
| Угрозы утечки видовой информации | Просмотр с помощью оптических (оптико-электронных) средств |
| Специальные электронные устройства съема видовой информации |
| Угрозы утечки информации по каналам ПЭМИН | ПЭМИН от технических средств и линий передачи информации |
| Наводки на цепи электропитания и линии связи, выходящие за пределы служебных помещений |
| Радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах технических средств |
| Радиоизлучения, формируемые в результате ВЧ облучения |
| Специальные электронные устройства съема |

Угрозы несанкционированного доступа с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирования, несанкционированного распространения), целостности (уничтожения, изменения) и доступности (блокирования) персональных данных, и включают в себя:

|  |  |
| --- | --- |
| угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения); | |
| угрозы непосредственного доступа реализуются с использованием программных и программно-аппаратных средств ввода/вывода | угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия |
| к информации и командам, хранящимся в базовой системе ввода/вывода (BIOS) с возможность перехвата управления загрузкой операционной системы и получением прав доверенного пользователя;  в операционную среду с возможностью выполнения несанкционированного доступа путем вызова штатных программ операционной системы или запуска специально разработанных программ;  в среду функционирования прикладных программ (например, к локальной системе управления базами данных);  непосредственно к информации пользователя и обусловлены возможностью нарушения ее конфиденциальности, целостности и доступности. | Наиболее часто реализуемые в настоящее время угрозы:  анализ сетевого трафика;  сканирование сети;  угроза выявления пароля;  подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа;  навязывание ложного маршрута сети;  внедрение ложного объекта сети;  отказ в обслуживании (частичное исчерпание ресурсов; полное исчерпание ресурсов; нарушение логической связности между атрибутами, данными, объектами; использование ошибок в программах);  удаленный запуск приложений (рассылка файлов, содержащих деструктивный исполняемый код, вирусное заражение; переполнение буфера серверного приложения; использование возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами). |
| угрозы создания нештатных режимов работы программных средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п. – угроза «Отказ в обслуживании» | |
| угрозы внедрения вредоносных программ (программно-математические воздействия). | |
| программных закладок;  классических программных (компьютерных) вирусов;  вредоносных программ, распространяющихся по сети (сетевых червей);  других вредоносных программ, предназначенных для осуществления НСД. | |

Возможны комбинированные угрозы, представляющие собой сочетание указанных угроз. Например, за счет внедрения вредоносных программ могут создаваться условия для НСД в операционную среду компьютера.

В «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» содержится описание результатов реализации угроз, например реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

* нарушению конфиденциальности (копирование, неправомерное распространение);
* нарушению целостности (уничтожение, изменение);
* нарушению доступности (блокирование).

С целью облегчения анализа угроз конкретным ИСПДн «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» содержит типовые модели угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных, для следующих видов систем:

|  |  |
| --- | --- |
| **Автоматизированное рабочее место** | |
| не имеющее подключения к сетям связи общего пользования и (или) сетям международного информационного обмена | имеющее подключения к сетям связи общего пользования и (или) сетям международного информационного обмена |
| **Локальная информационная система ПДн** | |
| не имеющая подключения к сетям связи общего пользования и (или) сетям международного информационного обмена | имеющая подключения к сетям связи общего пользования и (или) сетям международного информационного обмена |
| **Распределенная информационная система ПДн** | |
| не имеющая подключения к сетям связи общего пользования и (или) сетям международного информационного обмена | имеющая подключения к сетям связи общего пользования и (или) сетям международного информационного обмена |

Необходимо отметить, что **для специальных информационных систем типовые модели угроз не подходят. Для каждой из них строится своя модель на основе базовой модели.**

Определение актуальных угроз безопасности ПДн, обрабатываемым в ИСПДн, осуществляется на основании «Методики определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных».

В соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» угроза считается актуальной, если она представляет опасность и может быть реализована.

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

Уровень исходной защищенности определяется экспертным методом в соответствии с приведенной таблицей «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

|  |  |  |  |
| --- | --- | --- | --- |
| **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, поселка) |  |  | + |
| корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации |  | + |  |
| локальная 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:* | | | |
| ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн |  | + |  |
| ИСПДн, к которой имеют доступ 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 данной ИСПДн | + |  |  |
| *6. По уровню обобщения (обезличивания) ПДн:* | | | |
| ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.) | + |  |  |
| 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 (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн) |  |  | + |
| *7. По объему ПДн, которые* *предоставляются сторонним пользователям ИСПДн без предварительной обработки:* | | | |
| ИСПДн, предоставляющая всю БД с ПДн |  |  | + |
| ИСПДн, предоставляющая часть ПДн |  | + |  |
| ИСПДн, не предоставляющие никакой информации | + |  |  |

Исходная степень защищенности определяется следующим образом:

1. ИСПДн имеет *высокий (*Y1*=0)* 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).

2. ИСПДн имеет *средний (*Y1*=5)* уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные - низкому уровню защищенности.

3. ИСПДн имеет *низкую (*Y1*=10)* степень исходной защищенности, если не выполняется условия по пунктам 1 и 2.

Вероятность реализации каждой угрозы определяется экспертным путем и имеет четыре вербальных (числовых) градации этого показателя:

*маловероятно (*Y2*=*0*) ‑* отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

*низкая вероятность (*Y2*=*2*) ‑* объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

*средняя вероятность (*Y2*=*5*) –* объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

*высокая вероятность (*Y2*=*10*) ‑* объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

Далее рассчитывается коэффициент реализуемости каждой угрозы: Y=(Y1+Y2)/20

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

|  |  |
| --- | --- |
| **Значению коэффициента Y** | **Возможность реализации угрозы** |
| 0 ≤ Y ≤ 0,3 | Низкая |
| 0,3 < Y ≤ 0,6 | Средняя |
| 0,6 < Y ≤ 0,8 | Высокая |
| Y > 0,8 | Очень высокая |

Далее на основе опроса экспертов оценивается опасность каждой угрозы. При оценке опасности определяется вербальный показатель опасности для рассматриваемой ИСПДн. Этот показатель имеет три значения:

|  |  |
| --- | --- |
| **низкая опасность** | если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных |
| **средняя опасность** | если реализация угрозы может привести к негативным последствиям для субъектов персональных данных |
| **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, показанными в таблице.

|  |  |  |  |
| --- | --- | --- | --- |
| **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 |

Таким образом, формируется перечень актуальных угроз безопасности ПДн в ИСПДн и оформляется соответствующим документом (Акт определения уровня защищенности ИСПДн).