УТВЕРЖДАЮ

Директор ОАО «ЖЭУК «Южная»

_____ В.О.Очередниченко«

11 » 02 2013 г.

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ОАО «ЖЭУК «Южная»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Гражданским Кодексом Российской Федерации, Трудовым Кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», нормативно-методическими документами ФСТЭК России в сфере обработки персональных данных.

1.2 Цель разработки настоящего Положения – установление порядка организации и проведения работ по обеспечению безопасности персональных данных (далее – ПДн) в информационных системах персональных данных (далее – ИСПДн) ОАО «ЖЭУК «Южная» (далее – Общество) на протяжении всего жизненного цикла ИСПДн.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. В настоящем Положении используются следующие термины и их определения:

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

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания, если иное не предусмотрено федеральным законом.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс),

распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

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

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Угрозы безопасности персональных данных – 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, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых

уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

3. ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАНОСТИ ПДН

3.1 Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн, реализуемых в рамках создаваемой системы защиты персональных данных (СЗПДн).

3.2 Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн.

3.3 СЗПДн включает организационные меры и технические средства защиты информации (в том числе средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки, а также используемые в информационной системе информационные технологии).

3.4 СЗПДн в Обществе создается в три этапа:

Этап 1. Предпроектное обследование ИСПДн и разработка технического задания на создание СЗПДн.

Этап 2. Проектирование СЗПДн, закупка, установка, настройка и опытная эксплуатация необходимых средств защиты информации.

Этап 3. Ввод ИСПДн с СЗПДн в промышленную эксплуатацию.

3.5 Этап 1. Проведение предпроектного обследования и разработка технического задания на создание СЗПДн.

3.5.1. Создание в Обществе постоянно действующей Комиссии по обеспечению безопасности персональных данных.

3.5.2. Определение перечня субъектов персональных данных (физических лиц), ПДн которых обрабатываются в Обществе, перечня обрабатываемых ПДн и перечня документов, содержащих ПДн.

3.5.3. Определение перечня ИСПДн в Обществе и состава ПДн, обрабатываемых в ИСПДн. Перечень ИСПДн и обрабатываемых ПДн утверждается приказом директором Общества.

3.5.4. Определение целей обработки персональных данных – трудовые отношения с работниками Общества, организация управления и обслуживания жилищного фонда на территории муниципального образования «Город Йошкар - Ола».

3.5.5. Определение сроков обработки и хранения ПДн, исходя из требования, что ПДн не должны храниться дольше, чем этого требуют цели обработки этих ПДн, по достижению которых ПДн подлежат уничтожению. Определение перечня ПДн, цели обработки которых уже достигнуты.

3.5.6. Определение перечня используемых в ИСПДн (предлагаемых к использованию в ИСПДн) общесистемных и прикладных программных средств.

3.5.7. Определение режимов обработки ПДн в ИСПДн в целом и в отдельных компонентах.

3.5.8. Уточнение степени участия сотрудников Общества в обработке ПДн, характера их взаимодействия между собой. Утверждение перечня лиц, непосредственно осуществляющих обработку персональных данных в информационных системах Общества и вне информационных систем и лиц, имеющих доступ к ПДн, приказом директора Общества.

3.5.9. Назначение приказом директора Общества администратора безопасности ИСПДн для разработки и осуществления технических мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн. Для каждой ИСПДн может быть назначен отдельный администратор безопасности.

3.5.10. Разработка разрешительной системы доступа (матрицы доступа) пользователей ИСПДн к обрабатываемой на ИСПДн информации.

3.5.11. Определение границ контролируемой зоны путем издания соответствующего приказа директора Общества и условий расположения ИСПДн относительно границ контролируемой зоны.

3.5.12. Определение конфигурации и топологии ИСПДн в целом и их отдельных компонент, физических, функциональных и технологических связей как внутри этих систем, так и с другими системами различного уровня и назначения.

3.5.13. Определение технических средств и систем, используемых в ИСПДн, включая условия их расположения.

3.5.14. Разработка следующих организационно-распорядительных документов (далее ОРД), регламентирующих процесс обработки и защиты персональных данных:

– Положение о защите персональных данных, включая порядок взаимодействия с субъектами персональных данных, порядок взаимодействия с уполномоченными органами, порядок взаимодействия при передаче персональных данных третьим лицам, порядок обработки персональных данных и контроля за его соблюдением;

– Инструкция администратора безопасности ИСПДн;

– Инструкция пользователей ИСПДн по работе с персональными данными и средствами защиты информации;

– Раздел должностных инструкций работников Общества в части обеспечения безопасности ПДн при их обработке, включая установление персональной ответственности за нарушения правил обработки ПДн.

3.5.15. Классификация ИСПДн в соответствии с порядком проведения классификации информационных систем персональных данных, утвержденным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13.02.2008 № 55/86/20 (подготовка и утверждение акта классификации).

3.5.16. Определение угроз безопасности ПДн в конкретных условиях функционирования ИСПДн (разработка моделей угроз безопасности ПДн при их обработке в ИСПДн).

3.5.17. Формирование технического задания на разработку СЗПДн по результатам предпроектного обследования на основе нормативно-методических документов ФСТЭК России и ФСБ России с учетом установленного класса ИСПДн.

Техническое задание на разработку СЗПДн должно содержать:

– обоснование разработки СЗПДн;

– исходные данные создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах;

– класс ИСПДн;

– ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн, и приниматься в эксплуатацию ИСПДн;

– конкретизацию мероприятий и требований к СЗПДн;

– состав и содержание работ по этапам разработки и внедрения СЗПДн

– перечень предполагаемых к использованию сертифицированных средств защиты информации.

3.6 Этап 2. Проектирование СЗПДн, закупка, установка, настройка и опытная эксплуатация необходимых средств защиты информации.

3.6.1. Создание СЗПДн является необходимым условием обеспечения безопасности ПДн, в том случае, если существующие организационные и технические меры обеспечения безопасности не соответствуют требованиям к обеспечению безопасности ПДн для ИСПДн соответствующего класса и/или не покрывают всех угроз безопасности ПДн для данной ИСПДн.

3.6.2. Технические меры защиты ПДн предполагают использование программно-аппаратных средств защиты информации. При обработке ПДн с использованием средств автоматизации применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется в процессе предпроектного обследования информационных ресурсов Общества.

3.6.3. Средства защиты информации, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия, включая

сертификацию на соответствие требованиям по безопасности информации.

3.6.4. На стадии проектирования и создания СЗПДн для ИСПДн Общества проводятся следующие мероприятия:

– разработка (при необходимости) задания и проекта на строительные, строительно-монтажные работы (или реконструкцию) ИСПДн в соответствии с требованиями технического задания на разработку СЗПДн;

– разработка технического проекта СЗПДн;

– строительно-монтажные работы в соответствии с проектной документацией (при необходимости);

– приобретение (при необходимости), установка и настройка серийно выпускаемых технических средств обработки, передачи и хранения информации;

– разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями;

– приобретение, установка и настройка сертифицированных технических, программных и программно-технических средств защиты информации, в том числе (при необходимости) средств криптографической защиты информации;

– реализация разрешительной системы доступа пользователей ИСПДн к обрабатываемой на ИСПДн информации;

– определение подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации с их обучением по направлению обеспечения безопасности ПДн;

– подготовка эксплуатационной документации на используемые средства защиты информации;

– корректировка (дополнение) организационно-распорядительной документации в части защиты информации (положений, приказов, топологических схем, инструкций и других документов).

3.7 Этап 3. Ввод ИСПДн с СЗПДн в промышленную эксплуатацию.

3.7.1. На стадии ввода в ИСПДн (СЗПДн) осуществляются:

– опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;

– приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации.

– организация охраны и физической защиты помещений ИСПДн, и исключающих несанкционированный доступ к техническим средствам ИСПДн, хищение и нарушение работоспособности, хищение носителей информации.

4. ПРОВЕДЕНИЕ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Контроль за проведением работ по обеспечению безопасности ПДн осуществляет Комиссия по обеспечению безопасности персональных данных в виде методического руководства, участия в разработке требований по защите персональных данных, организации работ по выявлению возможных каналов утечки

информации, согласования выбора средств вычислительной техники и связи, технических и программных средств защиты, участия в оценке соответствия ИСПДн Общества требованиям безопасности ПДн.

4.2. При необходимости к проведению работ по обеспечению безопасности персональных данных могут привлекаться специализированные организации, имеющие лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации.

4.3. В соответствии с п. 5.2 Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденных руководством 8 Центра ФСБ России 21.02.2008 № 149/54-144, при необходимости использования при создании СЗПДн средств криптографической защиты информации к проведению работ по обеспечению безопасности персональных данных Обществу необходимо привлекать специализированные организации, имеющие лицензии ФСБ России на осуществление работ по распространению шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведения, составляющие государственную тайну, на осуществление технического обслуживания шифровальных (криптографических) средств, на осуществление работ по оказанию услуг в области шифрования информации, не содержащих сведений, составляющих государственную тайну.

5. РЕШЕНИЕ ВОПРОСОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПДН В ДИНАМИКЕ ИЗМЕНЕНИЯ ОБСТАНОВКИ И КОНТРОЛЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ

5.1. Модернизация СЗПДн для функционирующих ИСПДн Общества должна осуществляться в случае:

- изменения состава или структуры ИСПДн или технических особенностей ее построения (изменения состава или структуры программного обеспечения, технических средств обработки ПДн, топологии ИСПДн);
- изменения состава угроз безопасности ПДн в ИСПДн;
- изменения класса ИСПДн.

5.2. В целях определения необходимости доработки (модернизации) СЗПДн не реже одного раза в год Комиссией по обеспечению безопасности персональных данных должна проводиться проверка состава и структуры ИСПДн, состава угроз безопасности ПДн в ИСПДн и класса ИСПДн, соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией. Результаты проверки оформляются актом проверки и утверждаются директором Общества.

5.3. Разбирательство и составление заключений в обязательном порядке должно проводиться в случае выявления следующих фактов:

- несоблюдение условий хранения носителей персональных данных;
- использование средств защиты информации, которые могут привести к

нарушению заданного уровня безопасности (конфиденциальность/ целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных;

– нарушение заданного уровня безопасности ПДн (конфиденциальность/ целостность/доступность).

5.4. В процессе проведения разбирательства Комиссия по обеспечению безопасности персональных данных должна принять меры по предотвращению возможных негативных последствий допущенных нарушений, а по окончании проведения разбирательства – принять меры по предотвращению повторения подобных нарушений.