Приложение №10 к Положению
«О политике обработки персональных
данных в ООО «ЧТЗ-УРАЛТРАК»

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение о порядке организации и проведения работ по защите персональных данных ООО «ЧТЗ-УРАЛТРАК» (далее — Положение) определяет содержание и порядок осуществления мероприятий по защите персональных данных, обрабатываемых с использованием средств автоматизации в информационной системе персональных данных ООО «ЧТЗ-УРАЛТРАК» (далее – ИСПД).

1.2. Мероприятия по защите персональных данных являются составной частью управленческой и иной служебной деятельности ООО «ЧТЗ-УРАЛТРАК» (далее - Общества).

1.3. Защита персональных данных в ИСПД обеспечивается выполнением комплекса организационных мероприятий и применением средств защиты информации от несанкционированного доступа, программно-технических воздействий с целью нарушения целостности (модификации, уничтожения) и доступности информации в процессе ее обработки, передачи и хранения, а также обеспечения работоспособности технических средств.

1.4. Ответственность за своевременную организацию разработки и осуществление необходимых мероприятий по защите персональных данных в ИСПД возлагается на ответственного за обработку персональных данных в Обществе администратора безопасности информации.

1.5. Ответственность за выполнение требований по обеспечению информационной безопасности при проведении работ с персональными данными на автоматизированных рабочих местах ИСПДн, возлагается на руководителя подразделения Общества, в котором установлены автоматизированные рабочие места.

1.6. Лица, виновные в нарушении требований руководящих документов по вопросам защиты персональных данных, несут ответственность в соответствии с действующим законодательством Российской Федерации.

1.7. Настоящее Положение не исключает обязательного выполнения других действующих нормативных документов по вопросам защиты информации ограниченного доступа.

1.8. Положение предназначено для работников подразделений, занимающихся технической эксплуатацией и обеспечением информационной безопасности ИСПД, и пользователей ИСПД.

2. НОРМАТИВНО-МЕТОДИЧЕСКАЯ ДОКУМЕНТАЦИЯ

При организации и проведении работ по обеспечению безопасности персональных данных необходимо руководствоваться следующими нормативными и методическими документами:

- Конституция Российской Федерации;
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Указ Президента от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утверждены приказом № 21 ФСТЭК России от 18 февраля 2013 г;
- Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах (утв. заместителем директора ФСТЭК России 15 февраля 2008 г.);
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. заместителем директора ФСТЭК России 14 февраля 2008 г.);
- Специальные требования и рекомендации по технической защите персональных данных (утв. приказом Гостехкомиссии России от 30 февраля 2002 г. № 282).
-

3. ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИСПДн

3.1.Организационные мероприятия.

Организационные меры по защите персональных данных в ИСПД включают в себя следующие мероприятия:

- определение подразделений и лиц, ответственных за защиту информации в каждой ИСПД;
- определение перечней персональных данных;
- определение целей обработки персональных данных;
- определение сроков обработки и хранения персональных данных;
- определение круга лиц, допущенных к обработке персональных данных;
- организация доступа в помещения, где осуществляется обработка персональных данных;
- обучение работников, допущенных к обработке персональных данных, основам информационной безопасности;
- учет применяемых технических средств защиты информации;
- учет носителей персональных данных;
- разработка организационно-распорядительных документов.

3.1.1. Определение подразделений и лиц, ответственных за защиту персональных данных.

К организационным мерам защиты информации общего характера относится распределение работ, связанных с сопровождением системы защиты информации в ИСПД, между соответствующими подразделениями Общества. В проведении работ по сопровождению системы защиты информации в информационной системе Общества участвуют:

- отдел информационной безопасности;
- Подразделение подчиняющийся директору информационных технологий;
- подразделения Общества, участвующие в проведении работ с персональными данными на автоматизированных рабочих местах пользователей ИСПДн;
- специализированные предприятия, выполняющие специальное техническое обслуживание системы защиты информации в ИСПД.

Администраторы безопасности информации обеспечивают:

- организационно-методическое руководство работами по поддержанию уровня защиты информации, обрабатываемой в ИСПД, в соответствии с действующим нормами и требованиями;
- подготовку проектов распорядительных документов по вопросам администрирования в ИСПД;
- администрирование системы защиты информации ИСПД;
- привлечение специализированных предприятий к работам по специальному техническому обслуживанию системы защиты информации ИСПД;
- сопровождение работ, проводимых предприятиями, выполняющими специальное техническое обслуживание системы защиты информации ИСПД;
- проведение ежегодного контроля защищенности обрабатываемой информации;
- проведение повседневного контроля защищенности обрабатываемой информации;
- сопровождение любых работ на объекте, связанных с его техническими средствами и системами, оборудованием, ограждающими конструкциями, окнами, дверями помещения, проводимых подразделениями Общества или сторонними организациями;
- учет в соответствующих журналах учета машинных носителей информации.

отдел сетевого и системного администрирования Общества обеспечивает в соответствии со своими функциями выполнение работ в помещениях, в которых установлены технические средства ИСПДн, связанных с обслуживанием, ремонтом, заменой и т.п. закрепленных за ними технических средств (систем), оборудования, с учетом требований безопасности информации, обрабатываемой в ИСПД.

Работники подразделений Общества, участвующие в проведении работ на автоматизированных рабочих местах пользователей ИСПД с персональными данными обеспечивают:

- соблюдение установленного режима обработки персональных данных;
- режим прохода в помещения, в которых установлены технические средства ИСПД;
- осуществление работы на автоматизированных рабочих местах с установленной системой защиты информации от несанкционированного доступа;
- сохранность полученных в процессе работы персональных данных, машинных и других носителей информации, в том числе бракованных;
- неизменность размещения технических средств в помещениях, где установлено оборудование ИСПД.

Предприятия, выполняющие специальное техническое обслуживание системы защиты информации ИСПД, в рамках этого обслуживания осуществляют следующие работы:

- проведение плановой или внеплановой (при значительных изменениях компонентов ИСПД, его характеристик или элементов системы защиты информации) переаттестации ИСПД;
- подтверждение (при необходимости) эффективности системы защиты информации ИСПД после установки новых или ремонта ранее установленных основных технических средств, изменения состава общесистемного программного обеспечения автоматизированных рабочих станций;
- диагностику неисправностей, ремонт или замену (при необходимости) ранее установленных средств защиты, инструментальное и тестовое подтверждение (при необходимости) эффективности ИСПД после такого ремонта или замены;
- организацию (при необходимости) продления сертификатов Федеральной службы по техническому и экспортному контролю Российской Федерации (ФСТЭК России) на установленные средства защиты.

3.1.2.Регистрация событий безопасности.

События безопасности, подлежащие регистрации в информационной системе, и сроки их хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в информационной системе. Подлежат регистрации события безопасности, связанные с применением выбранных мер по защите информации в информационной системе. В информационной системе как минимум подлежат регистрации следующие события:

- вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы;
- подключение машинных носителей информации и вывод информации на носители информации;
- запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации.
- попытки доступа программных средств к определяемым администратором безопасности информации защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;
- попытки удаленного доступа.

Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

Минимальный срок хранения записей о событиях безопасности составляет 3 (три) месяца.

3.2.Технические мероприятия.

Технические меры защиты персональных данных в ИСПД предполагают использование программно-аппаратных средств защиты информации от несанкционированного доступа и средств антивирусной защиты. Настройка и сопровождение программно-аппаратных средств защиты информации от несанкционированного доступа и антивирусной защиты осуществляются администраторами безопасности информации.

3.2.1.Требования к техническим и программным средствам.

Технические и программные средства, используемые для обработки персональных данных, должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Средства защиты информации, применяемые в ИСПД, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

3.2.2.Необходимость создания системы защиты информации.

Создание системы защиты информации является необходимым условием обеспечения безопасности персональных данных в том случае, если существующие организационные и технические меры обеспечения безопасности не соответствуют требованиями к обеспечению безопасности персональных данных для ИСПД соответствующего класса и/или не исключают реализацию актуальных угроз безопасности информации в ИСПД.

3.2.3. Модернизация системы защиты информации.

Модернизация (доработка) системы защиты информации ИСПД должна проводиться в случае, если:

- изменился состав, или структура самой ИСПД, или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки персональных данных, топологии ЛВС);
- изменился состав угроз безопасности персональных данных в ИСПД;
- изменился необходимый уровень защищенности ИСПД.

Для определения необходимости доработки (модернизации) системы защиты информации ИСПД не реже одного раза в год должна проводиться проверка состава и структуры ИСПД, состава угроз безопасности персональных данных в ИСПД и уровня защищенности ИСПД. Проверка проводится администратором безопасности информации совместно с отделом сетевого и системного администрирования.

Порядок проведения модернизации и обязательные требования при внесении изменений в состав технических и программных средств ИСПД регламентируются отдельной инструкцией.

Врио генерального директора Е.Ю. Тихомирова