УТВЕРЖДАЮ
Генеральный директор
ООО «Управляющая компания «Холмсервис»

_____ И. И. Сидорова
«__» _____ 20__ г.
М. П.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

ООО «Управляющая компания «Холмсервис»

2014

1. Общие положения

1.1 Целью настоящей Политики является:

- обеспечение безопасности персональных данных (объектов защиты) ООО «Управляющая компания «Холмсервис» (далее – УК Холмсервис);
- защита персональных данных от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных;
- минимизация ущерба от возможной реализации угроз безопасности персональных данных.

Безопасность персональных данных достигается путем исключения 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 с ними. Персональные данные и связанные с ними ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности персональных данных. Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных. Состав персональных данных представлен в Перечне персональных данных, обрабатываемых в информационных системах персональных данных УК Холмсервис.

1.2 Требования настоящей Политики распространяются на всех сотрудников УК Холмсервис, участвующих в обработке ПДн, а также на все существующие, модернизируемые или вновь создаваемые ИСПДн УК Холмсервис.

2. Система защиты персональных данных

2.1 Система защиты персональных данных должна строиться с учетом требований:

- Федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Постановления Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г. № 1119;
- Постановления Правительства Российской Федерации «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 № 687;
- Методики определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 14.02.2008 заместителем директора ФСТЭК России);
- Базовой модели угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 15.02.2008 заместителем директора ФСТЭК России);
- «Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных приказом ФСТЭК России от 18.02.2013 № 21;
- Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных УК Холмсервис (далее – Модель угроз).

На основании Модели угроз и Акта оценки вреда субъекту ПДн должен быть определен необходимый уровень защищенности персональных данных. Уровень защищенности должен быть зафиксирован в Акте установления уровня защищенности персональных данных. На основании актуальных угроз безопасности персональных данных, описанных в Модели угроз, и требований

«Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных приказом ФСТЭК России от 18.02.2013 № 21, должно быть разработано техническое задание с описанием требований к техническим средствам и организационным мероприятиям, необходимым для обеспечения безопасности персональных данных, обрабатываемых в информационных системах персональных данных (далее - ИСПДн) УК Холмсервис.

Для каждой ИСПДн должен быть составлен и закреплен в Техническом паспорте список используемых технических и программных средств защиты информации и программного обеспечения, участвующего в обработке персональных данных, на всех элементах ИСПДн, в том числе:

- на АРМ пользователей ИСПДн;
- на серверах ИСПДн;
- на границах ЛВС УК Холмсервис;
- в каналах передачи данных в сети общего пользования и (или) международного информационного обмена.

Технический паспорт должен поддерживаться в актуальном состоянии. При изменении состава технических и программных средств защиты или элементов информационной системы соответствующие изменения должны быть внесены в Технический паспорт лицом, ответственным за обработку персональных данных, и утверждены генеральным директором УК Холмсервис.

В зависимости от уровня защищенности персональных данных и актуальных угроз, система защиты может включать следующие технические и программные средства:

- антивирусные средства для рабочих станций пользователей и серверов;
- средства межсетевого экранирования;
- средства обнаружения вторжений;
- средства криптографической защиты информации;
- средства защиты каналов связи;
- средства защиты от несанкционированного доступа к информации;
- средства затирания информации;
- средства анализа защищенности.

3. Требования к подсистемам системы защиты персональных данных

3.1 Система защиты персональных данных может включать в себя следующие подсистемы:

- идентификации и аутентификации субъектов доступа к объектам доступа;
- управления доступом субъектов доступа к объектам доступа;
- регистрации событий безопасности;
- антивирусной защиты;
- контроля (анализа) защищенности персональных данных;
- защиты технических средств.

Указанные подсистемы могут иметь различный функционал в зависимости от уровня защищенности персональных данных, определенного в Акте установления уровня защищенности персональных данных, обрабатываемых в ИСПДн.

3.1.1 В рамках подсистемы идентификации и аутентификации субъектов доступа к объектам доступа должны быть реализованы следующие меры:

- идентификация и аутентификация пользователей, являющихся работниками УК Холмсервис;
- управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;

- управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- защита обратной связи при вводе аутентификационной информации.

Подсистема должна реализовываться путем применения средств защиты информации от несанкционированного доступа и разработки организационно-распорядительной документации.

3.1.2 В рамках подсистемы управления доступом субъектов доступа к объектам доступа должны быть реализованы следующие меры:

- управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;
- реализация необходимых методов (дискреционный метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;
- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;
- ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);
- управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы);

Подсистема должна реализовываться путем применения средств защиты информации от несанкционированного доступа, средств межсетевого экранирования и разработки организационно-распорядительной документации.

3.1.3 В рамках подсистемы регистрации событий безопасности должны быть реализованы следующие меры:

- определение событий безопасности, подлежащих регистрации, и сроков их хранения;
- определение состава и содержания информации о событиях безопасности, подлежащих регистрации;
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- 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;
- мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;
- генерирование временных меток и (или) синхронизация системного времени в информационной системе;
- защита информации о событиях безопасности.

Подсистема должна реализовываться функционалом применяемых средств защиты информации, а также разработкой организационно-распорядительной документации.

3.1.4 В рамках подсистемы антивирусной защиты должны быть реализованы следующие меры:

- реализация антивирусной защиты;

– обновление базы данных признаков вредоносных компьютерных программ (вирусов);

Подсистема должна реализовываться путем внедрения антивирусного программного обеспечения на все элементы информационных систем персональных данных.

3.1.5 В рамках подсистемы контроля (анализа) защищенности должны быть реализованы следующие меры:

– контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.

Подсистема должна реализовываться применением программных средств контроля и (или) принятием организационных мер, регламентируемых соответствующей разработанной документацией.

3.1.6 В рамках подсистемы защиты технических средств должны быть реализованы следующие меры:

– 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;
– размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр

Подсистема должна реализовываться принятием организационных мер, регламентируемых соответствующей разработанной документацией.

4. Пользователи информационных систем персональных данных

В информационных системах персональных данных УК Холмсервис должны быть определены следующие группы пользователей, участвующих в обработке и хранении персональных данных:

– ответственный за обработку персональных данных в информационных системах персональных данных УК Холмсервис (далее – Ответственный);
– администратор безопасности информационных систем персональных данных УК Холмсервис (далее – Администратор безопасности);
– пользователь информационных систем персональных данных УК Холмсервис (далее – пользователь ИСПДн).

На основании этих категорий должны быть определены уровень доступа и возможности пользователей.

Данные о группах пользователей, уровне их доступа и информированности должны быть отражены в Положении о разграничении прав доступа к обрабатываемым персональным данным.

5. Требования к персоналу по обеспечению защиты персональных данных

Все сотрудники УК Холмсервис, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по обработке персональных данных и соблюдению принятого режима безопасности персональных данных.

При вступлении в должность нового сотрудника Ответственный обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите персональных данных, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования конкретной ИСПДн.

Сотрудник должен быть ознакомлен с требованиями настоящей Политики, принятыми процедурами работы с элементами конкретной ИСПДн и системой защиты персональных данных.

Сотрудники УК Холмсервис должны следовать установленным процедурам поддержания режима безопасности персональных данных при выборе и использовании паролей (если не используются технические средства аутентификации), определенным в Инструкции по организации парольной защиты в информационных системах персональных данных УК Холмсервис.

Сотрудники УК Холмсервис должны обеспечивать надлежащую защиту технических средств в ИСПДн, оставляемых без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности персональных данных и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них персональные данные.

Сотрудникам запрещается разглашать персональные данные, которые стали им известны при работе в ИСПДн УК Холмсервис, третьим лицам.

При работе с персональными данными в ИСПДн УК Холмсервис должны отсутствовать возможности просмотра персональных данных третьими лицами с мониторов автоматизированных рабочих мест или терминалов.

При завершении работы в ИСПДн сотрудники должны блокировать автоматизированные рабочие места с помощью встроенных в операционную систему средств или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники УК Холмсервис должны быть проинформированы об угрозах нарушения режима безопасности персональных данных и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности персональных данных.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, способных повлечь за собой угрозы безопасности персональных данных, а также о выявленных ими событиях, затрагивающих безопасность персональных данных, Ответственному и руководству организации.

6. Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн должны быть описаны в следующих документах:

- Инструкция ответственного за обработку персональных данных в УК Холмсервис;
- Инструкция администратора безопасности информационных систем персональных данных УК Холмсервис;
- Инструкция пользователя информационных систем персональных данных УК Холмсервис.

7. Ответственность сотрудников информационных систем персональных данных УК Холмсервис

Лица, виновные в нарушении требований законодательства о защите персональных данных, несут гражданскую, уголовную, административную, дисциплинарную и иную, предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство Российской Федерации позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей.

Администратор безопасности несет ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях пользователями ИСПДн правил, связанных с безопасностью персональных данных, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приведенные выше требования нормативных документов по защите информации должны быть отражены в должностных инструкциях сотрудников, осуществляющих обработку персональных данных в ИСПДн и должностных инструкциях сотрудников УК Холмсервис.

Положения о подразделениях УК Холмсервис, осуществляющих обработку персональных данных в ИСПДн, должны содержать сведения об ответственности их руководителей и сотрудников за разглашение и несанкционированную модификацию (искажение, фальсификацию) персональных данных, а также за неправомерное вмешательство в процессы их автоматизированной обработки.