Главное управление юстиции
Челябинской области

ПРИКАЗ

«30» января 2018г. № 11-о

г. Челябинск

Об утверждении Политики
информационной безопасности
Главного управления юстиции
Челябинской области

В целях исполнения законодательства Российской Федерации в области обеспечения информационной безопасности, а также обеспечения реализации мероприятий, утвержденных приказом начальника Главного управления юстиции Челябинской области (далее - Главного управления) от 27.02.2015г. № 64-о "О назначении ответственных должностных лиц за организацию и состояние защиты информации в Главном управлении юстиции Челябинской области и организации работ по технической защите информации при её обработке в информационных системах персональных данных" ПРИКАЗЫВАЮ:

1. Утвердить Политику информационной безопасности Главного управления согласно приложению.

2. Начальникам отделов (служб) Главного управления:

2.1. Руководствоваться в работе положениями Политики информационной безопасности для определения правил и обязанностей по доступу к защищаемым объектам и соблюдению принятого режима безопасности персональных данных в информационных системах персональных данных Главного управления.

2.2. Ознакомить сотрудников с положениями Политики информационной безопасности, утвержденной настоящим приказом.

3. Контроль за исполнением приказа оставляю за собой.

Начальник Главного управления В.П. Быков

Главное управление юстиции Челябинской области
ОГРН 1047423520286
ОТДЕЛ ГОСУДАРСТВЕННОЙ СЛУЖБЫ И КАДРОВ

Копия верна: старший инспектор отдела государственной службы и кадров Рядинская А.В.

Приложение к приказу
начальника Главного управления
юстиции Челябинской области
от «30» января 2018 г. № 11-о

ПОЛИТИКА
информационной безопасности
Главного управления юстиции Челябинской области

1. Введение

Политика информационной безопасности Главного управления юстиции Челябинской области (далее — Политика) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, в соответствии с требованиями Федерального закона «О персональных данных» и постановления Правительства Российской Федерации от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в системах персональных данных», на основании Приказа ФСТЭК России от «05» февраля 2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».

В Политике определены требования к персоналу информационных систем персональных данных (далее - ИСПДн), степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн Главного управления юстиции Челябинской области Челябинской области (далее - Управление).

2. Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты Управления от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

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.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

3. Основные термины и определения

В настоящем документе используются следующие термины и их определения:

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

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

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, 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.

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

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование,

распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

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, применяемые в информационных системах.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

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

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

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 невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

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

Обозначения и сокращения:

АРМ – автоматизированное рабочее место;

ИСПДн – информационная система персональных данных;

НСД – несанкционированный доступ;

ПДн – персональные данные;

УБПДн – угрозы безопасности персональных данных;

УК РФ – уголовный кодекс Российской Федерации

ЭВМ – электронная вычислительная машина

4. Категории персональных данных

Фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; адрес; семейное положение; социальное положение; имущественное положение; образование; профессия; доходы; паспортные данные, квалификация, ИНН, страховое свидетельство государственного пенсионного страхования, состав семьи, наименование категории гражданина, имеющего право на получение социальной выплаты за счет средств федерального бюджета.

5. Категории субъектов, персональные данные которых обрабатываются

Граждане, обратившиеся с жалобами, заявлениями; работники, с которыми заключены трудовые договоры, служебные контракты; граждане, направившие документы для участия в конкурсе на замещение вакантных должностей, в кадровый резерв.

6. Правовое основание обработки персональных данных

ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — Закон); ст. 7 Федерального закона от 02.05.2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»; глава 14 Трудового кодекса Российской Федерации от 30.12.2001 г. № 197-ФЗ; п. 3 ст. 9 Федерального закона от 01.04.1996 г. № 27-ФЗ (об индивидуальном персонифицированном учете в системе обязательного пенсионного страхования»; ст. 42 Федерального закона Российской Федерации от 27.07.2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации».

7. Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных

Персональные данные обрабатываются Оператором с использованием средств автоматизации и без использования таких средств. Оператором определен перечень действий (операций) с персональными данными при их обработке: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Обработка персональных данных: смешанная; с передачей по внутренней сети юридического лица; с передачей по сети Интернет.

8. Организационные меры по защите персональных данных

Приняты внутренние нормативные акты и изданы документы: Приказы о персональных данных и о назначении ответственных должностных лиц за организацию и состояние защиты информации в Управлении и организации работ по технической защите информации при ее обработке в информационных системах персональных данных; об утверждении перечня должностей Управления, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным; Положение о порядке организации и проведения работ по защите информации при ее обработке в информационных системах персональных данных, Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных; Положение об использовании средств защиты информации.

Разработаны: Регламент доступа в помещения со средствами информационных систем персональных данных, Инструкция по организации парольной защиты в информационных системах персональных данных, Инструкция по организации антивирусной защиты в информационных системах персональных данных, Инструкция по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам

информационных систем персональных данных; Инструкция по учету, хранению и уничтожению съемных носителей персональных данных; Инструкцию администратора информационной безопасности информационных систем персональных данных; Инструкцию по резервированию защищаемой информации в информационных системах персональных данных; Инструкцию по установке, модификации программного обеспечения и техническому обслуживанию средств вычислительной техники информационных систем персональных данных.

Утвержден акт классификации ИСПДн.

9. Сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации

Построена система защиты персональных данных с реализацией организационных и технических мер защиты; организован режим обеспечения безопасности помещений, в которых размещены информационные системы; обеспечивается сохранность носителей ПДн; утвержден перечень лиц, допуск которых к ПДн, обрабатываемым в информационной системе персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей; используются сертифицированные уполномоченными органами средства защиты информации; назначено должностное лицо, ответственное за обеспечение безопасности ПДн в ИСПДн.

10. Требования к пользователям ИСПДн

Все работники Управления, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

Работники Управления, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Работники Управления должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Работники Управления должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

Запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Управления, третьим лицам.

При работе с ПДн в ИСПДн работники Управления обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИСПДн работники Управления обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Работники Управления обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

11. Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн отражены в следующих документах:

Приказы об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, об утверждении перечня должностей Управления, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным.

12. Ответственность пользователей ИСПДн

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство РФ 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 (статьи 272, 273 и 274 УК РФ).

При нарушениях работниками Управления – пользователями ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

13. Заключительные положения

Настоящая Политика является внутренним документом Управления, общедоступной и подлежит размещению на официальном сайте Управления.

Управление имеет право вносить изменения в настоящую Политику. Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных.

Контроль исполнения требований настоящей Политики осуществляется ответственным за организацию обработки персональных данных в Управлении.