Российская Федерация
Муниципальное казенное учреждение
«Централизованная бухгалтерия
города Усолье-Сибирское»
(МКУ «ЦБ г. Усолье-Сибирское»)
ПРИКАЗ
19.12.2017г. № 331
г. Усолье-Сибирское

«Об утверждении Политики
обеспечения безопасности
удаленного доступа в МКУ «ЦБ г. Усолье-Сибирское»

В целях исполнения законодательства Российской Федерации в области обеспечения информационной безопасности

ПРИКАЗЫВАЮ:

1. Утвердить Политику обеспечения безопасности удаленного доступа в МКУ «ЦБ г. Усолье-Сибирское» (Приложение №1).
2. Заместителю директора Левиной О.А. организовать размещение данного приказа на странице официального сайта МКУ «ЦБ г. Усолье-Сибирское».
3. Инспектору по кадрам Спешиловой Т.Н. организовать ознакомление сотрудников МКУ «ЦБ г. Усолье-Сибирское», в том числе вновь поступающих на работу с настоящим приказом.
4. Контроль за исполнением настоящего приказа оставляю за собой.

Директор МКУ «ЦБ г. Усолье-Сибирское» Л.Ф.Шевнина

Приложение № 1
к приказу МКУ «ЦБ
г.Усолье-Сибирское»
от 19.12.2017г. № 331

Политика
обеспечения безопасности удаленного доступа
МКУ «ЦБ г. Усолье-Сибирское»

1. Введение

Настоящая Политика информационной безопасности (далее - Политика) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных МКУ «ЦБ города Усолье-Сибирское» (далее - Учреждение) изложенных в Концепции информационной безопасности ИСПДн Учреждения.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных» и Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2. Термины и сокращения

В настоящем документе используются следующие термины и их определения:

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

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.

Персональные данные (ПДн) – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Угрозы безопасности персональных данных (УБПДн) – 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

3. Общие положения

3.1. Целью настоящей Политики является обеспечение безопасности объектов защиты ИСПДн в МКУ «ЦБ города Усолье-Сибирское» от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн) информационной системы.

3.2. 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.

3.3. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

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

3.5. Состав объектов защиты представлен в Перечне персональных данных обрабатываемых в Учреждении, утверждаемом Руководителем Учреждения.

4. Область действия

4.1. Требования настоящей Политики распространяются на всех работников Учреждения, а также всех прочих лиц, допущенных к работам на территории Учреждения (подрядчики, аудиторы и т.п.).

5. Политика обеспечения безопасности удаленного доступа

5.1. Работникам Учреждения запрещено осуществление противоправных действий, включая деятельность по получению несанкционированного доступа к любой АС; нанесение ущерба и нарушение работы АС; перехват паролей или иной способ получения паролей, ключевой информации или иных механизмов доступа, которые могут быть использованы для несанкционированного доступа.

5.2. Программное обеспечение, предполагающее использование механизмов разделения доступа или подразумевающее индивидуальную ответственность работника за осуществляемые действия, должно использовать механизм контроля доступа, с идентификацией и авторизацией пользователя с помощью, как минимум пароля, отвечающего требованиям политики парольной защиты.

5.3. Настройка доступа ко всем информационным ресурсам Учреждения должна быть по умолчанию направлена на предотвращение к ним любого несанкционированного доступа.

5.4. Если система контроля доступа АРМ, корпоративной сети или автоматизированной системе вышла из строя, то по умолчанию доступ пользователей должен быть запрещен.

5.5. Доступ к информационным ресурсам Учреждения должен осуществляться согласно разработанной и утвержденной руководителем «Матрицы доступа», составленной на основании должностных обязанностей работников Учреждения и отчета о проведенной внутренней проверки.
5.6. Любое изменение в правах доступа к информационным ресурсам Учреждения должно быть обосновано выполнением должностных обязанностей, утверждено и направлено администратору информационной безопасности.
5.7. При увольнении работников Учреждения или изменении их должностных обязанностей, лица, уполномоченные на предоставление прав доступа, должны быть письменно проинформированы в трехдневный срок, после чего внести соответствующие изменения в систему контроля доступа и «Матрицу доступа».
5.8. Для установления персональной ответственности идентификатор учетной записи пользователя в любой информационной системе должен однозначно соответствовать отдельному работнику.
5.9. Компьютеры и терминалы должны быть оставлены в состоянии выполненного выхода из системы или с запирающим механизмом экрана или клавиатуры, управляемым паролем, маркером или подобным механизмом аутентификации пользователя, когда они находятся без присмотра, и должны быть защищены блокировкой клавиатуры, паролями или другими средствами управления, когда не используются.
5.10. Для доступа к АРМ и корпоративной сети Учреждения у каждого пользователя должны быть уникальный набор из идентификатора учетной записи и пароля. Запрещено создание идентификатора учетной записи, используемого группой лиц.
5.10.1. Использование идентификатора учетной записи пользователя после увольнения или прекращения использования информационных ресурсов Учреждения запрещено.
5.10.2. При предоставлении идентификатора учетной записи сторонним организациям необходимо заключение соглашений, подтверждающих обязательства сторонних организаций соблюдать требования НПА РФ и организационно-распорядительных документов Учреждения, подписанные уполномоченными лицами.
5.10.3. При прекращении необходимости использования сторонними организациям идентификатора учетной записи, лица, уполномоченные на предоставление прав доступа, должны быть письменно проинформированы в однодневный срок, после чего должны быть внесены соответствующие изменения в систему контроля доступа и «Матрицу доступа».
5.10.4. Для всех лиц, не являющихся служащими Учреждения, но для выполнения обязательств которых, необходимо предоставление доступа к АРМ и корпоративной сети Учреждения, должен быть сформирован идентификатор учетной записи, действующий только на период выполнения лицом своих обязательств. В случае, если срок выполнения обязательств не определен, то срок действия идентификатора учетной записи должен составлять 60 дней.
5.10.5. Пользователям запрещено использование идентификаторов учетных записей и паролей, используемых для получения доступа к информационным ресурсам Учреждения, для идентификации и аутентификации на публичных ресурсах сетей общего пользования.

5.11. Все автоматизированные системы и технические средства должны поддерживать специальный тип учетной записи, позволяющий производить любые поддерживаемые настройки и изменения, включая изменения в системе обеспечения безопасности.

5.11.1. Количество таких типов учетных записей должно быть максимально ограничено и предоставлено только тем пользователям, которым это необходимо для осуществления должностных обязанностей с учетом соблюдения требований НПА РФ и организационно-распорядительных документов Учреждения.

5.11.2. Таким лицам должны быть предоставлены как минимум два типа учетных записей, одна – специальный тип учетной записи, другая – ограниченный тип учетной записи для повседневной работы, не требующей изменения настроек АС.

5.11.3. Удаленное администрирование любых технических устройств в корпоративной сети Учреждения, при котором осуществляется передача информации через сети общего пользования, запрещено.

5.12. АРМ должны переводиться в режим запроса пароля после определенного периода бездействия или при отсутствии возможности контроля пользователем доступа к АРМ.

5.12.1. При наличии технической возможности, средства контроля доступа должны быть настроены на временную блокировку доступа к ним, после трехкратной попытки получения доступа, и уведомления уполномоченных лиц о таковых фактах.

5.12.2. При наличии технической возможности удаленные подключения к автоматизированной системе должны автоматически отключаться после определенного времени неактивности такого подключения.

5.13. Пользователям запрещено собирать и копировать информацию с информационных ресурсов, если это не обусловлено выполнением должностных обязанностей. При наличии технической возможности используемые системы контроля доступа должны предупреждать возможность таких действий и информировать о таких попытках.

5.14. Программисты и другой технический персонал не должны устанавливать и использовать программное обеспечение, направленное на обход установленных механизмов доступа или получение сведений для несанкционированного доступа. Если использование такого программного обеспечения необходимо для выполнения должностных обязанностей, то его использование должно осуществляться только уполномоченными лицами.