Российская Федерация
Муниципальное казенное учреждение
«Централизованная бухгалтерия
города Усолье-Сибирское»
(МКУ «ЦБ г. Усолье-Сибирское»)

ПРИКАЗ

19.12.2017г. № 335

г. Усолье-Сибирское

«Об утверждении Политики
управления доступом к ресурсам
корпоративной сети в МКУ «ЦБ г. Усолье-Сибирское»

В целях исполнения законодательства Российской Федерации в области обеспечения информационной безопасности

ПРИКАЗЫВАЮ:

1. Утвердить Политику управления доступом к ресурсам корпоративной сети 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. № 335

Политика
управления доступом к ресурсам корпортивной сети
в МКУ «ЦБ г. Усолье-Сибирское»

1. ОПРЕДЕЛЕНИЯ

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.
Безопасность персональных данных – состояние защищенности персональных данных, обрабатываемых и хранимых на бумажных и электронных носителях, и в информационных системах персональных данных, характеризуемое способностью обеспечить конфиденциальность, целостность и доступность персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

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.

Информация ограниченного доступа – любая информация,

отнесенная к конфиденциальной информации, коммерческой тайне, персональным данным, служебной тайне или иная информация, доступ к которой ограничен согласно организационно-распорядительным документам Учреждения в соответствии с нормативно-правовыми актами Российской Федерации.

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.

Компьютерный вирус – разновидность компьютерных программ, отличительной особенностью которых является способность к размножению, а также возможность выполнения произвольных действий, без ведома пользователя.

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.

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

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

2. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АС – автоматизированная система
АРМ – автоматизированное рабочее место
ИСПДн – информационная система персональных данных
КЗ – контролируемая зона
КС – корпоративная сеть Учреждения
НПА РФ – нормативные правовые акты Российской Федерации
НСД – несанкционированный доступ
ОС – операционная система
ПДн – персональные данные
ПО – программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
СЗИ – средства защиты информации

СОП – сеть общего пользования

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. Целью настоящей Политики является обеспечение безопасности объектов защиты Учреждения от всех видов угроз: внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн.

Безопасность ПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий.

3.2. Политика устанавливает правила:

– обеспечения сохранности имущества Учреждения и его эксплуатации, необходимого для обеспечения информационной безопасности;

– предотвращения, обнаружения и устранения последствий компьютерных вирусов и вредоносных программ;

– получения доступа к сетям общего пользования, правил работы в них, ограничений по их использованию, обеспечению безопасности при работе с ними и действия при ее нарушении;

– использования электронной почты и т.д.

Информация и связанные с ней ресурсы должны быть доступны только для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозы ПДн и предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных. Состав объектов защиты определяется в Перечне персональных данных, подлежащих защите.

4. ОБЛАСТЬ ДЕЙСТВИЯ

4.1. Требования настоящей Политики распространяются на всех сотрудников Учреждения (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

4.2. Сотрудникам Учреждения запрещено осуществление противоправных действий:

– по получению несанкционированного доступа к любой АС;

– по нанесению ущерба и нарушению работы АС;

– по перехвату паролей или иному способу получения паролей, ключевой информации или иных механизмов доступа, которые могут быть использованы для НСД.

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

Доступ к информации ограниченного доступа должен соответствовать требованиям НПА РФ и организационно-распорядительных документов Учреждения. Меры безопасности, используемые на АРМ и в КС, должны быть просты для использования, управления и аудита.

Настройка доступа ко всем информационным ресурсам Учреждения должна быть по умолчанию направлена на предотвращение к ним любого НСД. Если система контроля доступа АРМ, КС или АС вышла из строя, то доступ пользователей должен быть запрещен до решения проблемы. До предоставления прав доступа к информационным ресурсам Учреждения, пользователь должен быть ознакомлен под роспись с организационно-распорядительными документами Учреждения, регламентирующими работу с конкретными информационными ресурсами. В случаях, когда это определено необходимостью или требованиями НПА РФ или организационно-распорядительными документами Учреждения должен быть проведен дополнительный инструктаж или обучение. Факт проведения инструктажа или обучения должен быть закреплен в соответствии с требованиями документов, обуславливающих их проведение. В случаях, когда это определено НПА РФ и организационно- распорядительными документами Учреждения, сотрудник помимо ознакомления, должен письменно подтвердить свое обязательство выполнять требования документов.

5. Общие правила доступа к КС

5.1. Доступ к информационным ресурсам Учреждения должен осуществляться согласно разработанной и утвержденной приказом «Матрицы доступа», составленной на основании должностных обязанностей сотрудников Учреждения и отчета о проведенной внутренней проверки. В «Матрице доступа» должны быть отражены все пользователи Учреждения, имеющие доступ к информационным ресурсам Учреждения. Любое изменение в правах доступа к информационным ресурсам Учреждения должно быть обосновано

выполнением должностных обязанностей, утверждено и направлено администраторам информационной безопасности, корпоративной сети и АС.

5.2. В Учреждении должна вестись и своевременно обновляться «Матрица доступа». При увольнении сотрудников 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». Идентификатор учетной записи Идентификатор учетной записи пользователя должен быть составлен таким образом, чтобы не позволить не уполномоченным лицам установить личность пользователя.

5.3. Для установления персональной ответственности идентификатор учетной записи пользователя в любой АС должен однозначно соответствовать отдельному сотруднику.

5.4. Для доступа к АРМ и КС у каждого пользователя должны быть уникальный набор из идентификатора учетной записи и пароля. Запрещено создание идентификатора учетной записи, используемого группой лиц. Использование идентификатора учетной записи пользователя после увольнения или прекращения использования информационных ресурсов Учреждения запрещено.

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. При прекращении необходимости использования сторонними организациями 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».

5.5. Для всех лиц, не являющихся сотрудниками Учреждения, но для выполнения обязательств которых, необходимо предоставление доступа к АРМ и КС 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 15 дней. 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.

5.6. Учетные записи специальных типов Все АС и технические средства, используемые в них, должны поддерживать специальный тип учетной записи, позволяющий производить любые поддерживаемые настройки и изменения, включая изменения в системе обеспечения безопасности. 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.

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.

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

5.8. Требования по настройке системы управления доступом АРМ должны переводиться в режим запроса пароля после определенного периода бездействия или при отсутствии возможности контроля пользователем доступа к АРМ. 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. При наличии технической возможности удаленные подключения к АС должны автоматически отключаться после 30 минут неактивности подключения.

5.9. Сотрудникам 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. Требования безопасности по использованию системы управления доступа Программисты и другой технический персонал не должны устанавливать и использовать ПО, направленное на обход установленных механизмов доступа или получение сведений для НСД. Если использование такого ПО необходимо для выполнения должностных обязанностей, то его использование должно осуществляться только уполномоченными лицами.