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

ПРИКАЗ

19.12.2017г. № 338

г. Усолье-Сибирское

« Об утверждении Политики
антивирусной защиты
в МКУ «ЦБ г. Усолье-Сибирское»

В целях исполнения законодательства Российской Федерации в области обеспечения информационной безопасности

ПРИКАЗЫВАЮ:

1. Утвердить Политику антивирусной защиты 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. № 338

Политика
антивирусной защиты
в МКУ «ЦБ г. Усолье-Сибирское»

1. Общие положения

1.1. Политика антивирусной защиты (далее – Политика) МКУ «Централизованная бухгалтерия города Усолье-Сибирское» (далее - Учреждение) разработана в соответствии с Концепцией безопасности информации Учреждения, и определяет требования к организации защиты информационно-вычислительной сети (далее – ИВС) от вредоносных программ, с целью предотвращения потери (искажения, перехвата) информации, заражения программного обеспечения, перегрузки и повреждения оборудования ИВС.

1.2. Политика является руководящим документом, единым для всего Учреждения и обязательным для выполнения всеми работниками Учреждения.

1.3. Требования данной политики не распространяются напрямую на используемые в Учреждении компьютерные системы контроля и управления доступом (СКУД), но должны быть учтены во внутренних документах по режиму и экономической безопасности регламентирующих работу этих систем.

2. Определения

В настоящем документе используются следующие термины и их определения:

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для

осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вредоносный код – содержащаяся в любых файлах последовательность символов, результат исполнения которых позволяет отнести ее к компьютерным вирусам или вредоносным программам.

3. Объекты антивирусной защиты.

3.1. К объектам антивирусной защиты относятся:

- Серверы ИВС;
- Компьютеры (ноутбуки), принадлежащие, подключенные или периодически подключаемые к ИВС;
- Компьютеры (ноутбуки), не подключенные к ИВС, но по специфике их использования предполагается копирование (перенос) информации, содержащейся в них, на ресурсы ИВС или обратно;
- Компьютеры (ноутбуки), принадлежащие третьим лицам и подключаемые к ИВС в рамках заключенных договоров на выполнение работ (оказания услуг);
- Шлюз (шлюзы), соединяющий ИВС с сетью Интернет и другими сетями;
- Корпоративная система электронной почты.

Антивирусное ПО должно быть установлено и функционировать в штатном режиме на всех компьютерах, выполняющих функции серверов КС, на всех АРМ отдельно стоящих и подключенных к КС и на всех портативных компьютерах.

Не допускается изменение настроек системы антивирусной защиты, в части оповещения о нахождении компьютерных вирусов или вредоносных программ, в результате действия которых уменьшается эффективность работы АС.

Обновления баз системы антивирусной защиты должно производиться регулярно.

Построение системы антивирусной защиты должно предусматривать возможность обновления ее антивирусных баз и компонентов производителем по мере их создания. В случае невозможности такого построения системы (например, отдельно стоящие АРМ не подключенные к каким-либо сетям), обновление системы

антивирусной защиты должно производиться с регулярностью, обеспечивающей ее эффективное функционирование.
Запрещается отключение системы антивирусной защиты, за исключением случаев проведения тестирования программного обеспечения и иных тестов, проводимых уполномоченными сотрудниками Учреждения.

3.2. Предотвращение выполнения вредоносного кода

Структурные подразделения Учреждения обязаны проводить сканирование своих информационных ресурсов, а также всех подключенных АРМ на наличие компьютерных вирусов и вредоносных программ. Файлы, полученные любым образом, с любых носителей информации или сетей общего пользования должны быть проверены на наличие вредоносного кода.
Подключения к АРМ незарегистрированных электронных носителей информации (дискеты, компакт-диски, съемные жесткие диски, сотовые телефоны, карманные персональные компьютеры, фотоаппараты и иные носители информации) разрешено с обязательной проверкой «по требованию» таких носителей информации на наличие компьютерных вирусов и вредоносных программ.
На АРМ, с установленной операционной системой Windows любых версий, должна быть отключена функция автоматического исполнения операционной системой файла autorun.inf на электронных носителях информации. В случае получения файлов, проверка которых в исходном состоянии невозможна (например, файлы содержат архивы, не поддерживаемые системой антивирусной защиты, файлы прошли криптографическое преобразование и т.п.), необходимо на АРМ, не подключенном к КС, привести данные файлы к состоянию пригодному для проверки на наличие вредоносного кода, осуществить такую проверку, после чего принимать решение о возможности использования данных файлов.
Пользователи, которые в соответствии с должностными обязанностями используют служебные мобильные устройства к компьютерам, должны в обязательном порядке соблюдать требования настоящей Политики в их отношении. Все файлы, передаваемые третьим лицам, должны быть проверены на наличие вредоносного кода системой антивирусной защиты до их передачи. Любые намеренные попытки написания, компиляции, хранения, запуска, пропагандирования или распространения пользователями компьютерных вирусов или

вредоносных программ, а также иного кода, предназначенного для саморазмножения, нанесения ущерба или снижения производительности АС Учреждения, запрещены.

3.3. Обнаружение вредоносного кода

В случае обнаружения системой антивирусной защиты компьютерного вируса или вредоносной программы пользователь обязан выключить компьютер и сообщить об этом администратору информационной безопасности. О любом инциденте, связанном с выявлением компьютерного вируса или вредоносных программ, на АРМ или портативном компьютере, подключаемом к КС, должно быть сообщено администратору информационной безопасности.

Самостоятельные попытки пользователя по удалению компьютерного вируса или вредоносной программы запрещены.

В случае обнаружения в КС компьютерных вирусов или вредоносных программ в сообщениях электронной почты, систем обмена сообщениями и т.п., данные сообщения будут удалены.

Файлы, содержащие вредоносный код, должны быть удалены системой антивирусной защиты.