Муниципальное общеобразовательное учреждение
«Беседская основная общеобразовательная школа»
(МОУ «Беседская ООШ»)

Согласовано
Председатель
трудового коллектива
Кротова И.П. _____

Утверждено
приказом
№ 116 от 31. 08.2017

Инструкции по организации парольной и антивирусной защиты

Инструкция по организации парольной защиты

Данная инструкция призвана регламентировать организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в автоматизированной системе организации, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах АС и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на сотрудников подразделения обеспечения безопасности информации (ПОБИ) - администраторов средств защиты, содержащих механизмы идентификации и аутентификации (подтверждения подлинности) пользователей по значениям паролей.

Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями автоматизированной системы самостоятельно с учетом следующих требований:

длина пароля должна быть не менее установленной (обычно 6-8 символов);

в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

при смене пароля новое значение должно отличаться от предыдущего не менее чем в заданном числе (например в 6-ти) позициях;

личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных сотрудников ПОБИ. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления самих уполномоченных сотрудников ПОБИ, а также ответственных за информационную безопасность в подразделениях с паролями других сотрудников подразделений организации (исполнителей).

При наличии технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами своих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение ответственному за информационную безопасность подразделения

(руководителю своего подразделения). Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при их наличии у исполнителей), либо печать уполномоченного представителя службы обеспечения безопасности информации (ПОБИ).

Полная плановая смена паролей пользователей должна проводиться регулярно, например, не реже одного раза в месяц.

Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и т.п.) должна производиться администраторами соответствующих средств защиты в соответствии с «Инструкцией по внесению изменений в списки пользователей АС и наделению их полномочиями доступа к ресурсам системы» немедленно после окончания последнего сеанса работы данного пользователя с системой.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем АС.

В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры по внеплановой смене паролей (в зависимости от полномочий владельца скомпрометированного пароля).

Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у ответственного за информационную безопасность или руководителя подразделения в опечатанном личной печатью пенале (возможно вместе с персональными ключевыми дискетами и идентификатором Touch Memory).

Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственных за информационную безопасность в подразделениях (руководителей подразделений), периодический контроль - возлагается на сотрудников ПОБИ - администраторов средств парольной защиты.

Инструкция по организации антивирусной защиты

Настоящая Инструкция определяет требования к организации защиты АС организации от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих АС, за их выполнение.

К использованию в организации допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств, рекомендованные к применению отделами автоматизации и безопасности информации.

В случае необходимости использования антивирусных средств, не вошедших в перечень рекомендованных, их применение необходимо согласовать с отделами автоматизации и безопасности информации.

Установка средств антивирусного контроля на компьютерах на серверах и рабочих станциях АС осуществляется уполномоченными сотрудниками отдела автоматизации в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств АС».

Настройка параметров средств антивирусного контроля осуществляется сотрудниками ОА в соответствии руководствами по применению конкретных антивирусных средств.

Применение средств антивирусного контроля

Антивирусный контроль всех дисков и файлов рабочих станций должен проводиться ежедневно в начале работы при загрузке компьютера (для серверов - при перезапуске) в автоматическом режиме.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD - ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере или, при условии начальной загрузки операционной системы в оперативную память компьютера с заведомо "чистой" (не зараженной вирусами) и защищенной от записи системной дискеты, - на любом другом компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

Установка (изменение) системного и прикладного программного обеспечения осуществляется на основании «Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы организации».

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка:

• на защищаемых серверах и РС - ответственным за обеспечение информационной безопасности подразделения;

• на других серверах и РС АС не требующих защиты, - лицом, установившим (изменившим) программное обеспечение, - в присутствии и под контролем руководителя данного подразделения или сотрудника, им уполномоченного.

Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в специальном журнале подразделения за подписью лица, установившего (изменившего) программное обеспечение, и лица, его контролировавшего.

Действия при обнаружении вирусов

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник подразделения самостоятельно или вместе с ответственным за обеспечение безопасности информации подразделения (технологического участка) должен провести внеочередной антивирусный контроль своей рабочей станции. При необходимости привлечь специалистов ОА для определения ими факта наличия или отсутствия компьютерного вируса.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

• приостановить работу;

• немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и ответственного за обеспечение информационной безопасности своего подразделения, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
• совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
• провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь специалистов ОА);
• в случае обнаружения нового вируса, не поддающегося лечению ' применяемыми антивирусными средствами, передать зараженный вирусом файл на гибком магнитном диске в ОА для дальнейшей отправки его в организацию, с которой заключен договор на антивирусную поддержку;
• по факту обнаружения зараженных вирусом файлов составить служебную записку в отдел обеспечения безопасности информации, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

Ответственность

Ответственность за организацию антивирусного контроля в подразделении, эксплуатирующем подсистему АС, в соответствии с требованиями настоящей Инструкции возлагается на руководителя подразделения.

Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение безопасности информации и всех сотрудников подразделения, являющихся пользователями АС.