« Утверждаю»
Заведующий
МДОУ ДС КВ № 32 г. Ейска МО Ейский район
_____ А. А.Золотарева
"10"апреля 2015г.

ИНСТРУКЦИЯ
по защите от воздействия программных вирусов в информационных ресурсах, содержащих персональные данные МДОУ ДСКВ г.Ейска МО Ейский район

Защита информации от воздействия программных вирусов на ПК (рабочая станция, сервер, специализированный компьютер) достигается:

а) проведением организационных мероприятий по защите информации;

б) применением программных и технических средств защиты информации;

в) строгим соблюдением правил приема, ввода в эксплуатацию и эксплуатации на ПК программных средств общего и специального назначения, а также средств защиты информации;

г) контролем за соблюдением требований по защите информации от воздействия программных вирусов ответственными и должностными лицами;

Непосредственную ответственность за использование антивирусной защиты на ПК несут пользователи.

Должностные лица (пользователи), обрабатывающие информацию на средствах вычислительной техники, обязаны строго соблюдать установленные правила применения средств антивирусной защиты при работе на средствах вычислительной техники.

На каждом ПК должен быть установлен антивирусный пакет. Эксплуатация ПК без установленного на нем антивирусного пакета запрещена, кроме случаев предусмотренных специальных режимов эксплуатации этого ПК.

Установка антивирусного пакета осуществляется ответственным по установке базового программного обеспечения.

Средства защиты информации от воздействия программных вирусов и обновляемые антивирусные базы, используемые для установки на ПК, записываются на съемные машинные носители информации и общедоступные ресурсы (диски серверов). Обновление антивирусных баз осуществляется по графику обновления антивирусных баз.

Порядок применения средств антивирусной защиты устанавливается в соответствии с требованиями документации на средства антивирусной защиты и должен включать следующие виды работ:

а) обязательный входной контроль на отсутствие программных вирусов всех поступающих машинных носителей информации, а также поступающих по

каналам связи вычислительных сетей информационных ресурсов в виде файлов;

б) периодическую проверку пользователями несъемных магнитных носителей информации и обязательную проверку используемых в работе съемных носителей информации перед началом работы с ними на отсутствие программных вирусов;

в) внеплановую проверку носителей информации на отсутствие программных вирусов в случае подозрения на наличие программного вируса, либо по требованию ответственного по защите информации;

г) восстановление работоспособности программных средств и данных в случае их повреждения программными вирусами.

В случае обнаружения программных вирусов или факта несанкционированной модификации (уничтожения) информации пользователь обязан немедленно прекратить все работы, доложить о случившемся ответственному по защите информации и принять меры по локализации и удалению программных вирусов с помощью имеющихся средств антивирусной защиты.

Виновные в заражении подсистем ПК программными вирусами, работа которых привела к порче (модификации/удалению) информации или установленного программного обеспечения ПК или сбоям в работе ПК, несут ответственность в соответствии с действующим законодательством.

Ликвидация последствий воздействия программных вирусов осуществляется пользователями и системными администраторами организации.

О факте обнаружения программных вирусов сообщается в организацию отправитель, от которой поступили машинные носители информации, для принятия мер по локализации и устранению программных вирусов.

До полного уничтожения программных вирусов использование зараженных машинных носителей информации (МНИ) и вычислительной техники, на которых эти МНИ установлены (используются), запрещено.

Отключать установленные на ПК средства антивирусной защиты запрещается.

Ознакомлен:

Ведяева Е.М.

(дата) (подпись) (Ф.И.О.)

«Утверждаю»
Заведующий
МДОУ ДС КВ № 32 г. Ейска МО Ейский район

_____ А. А. Золотарева
"10"апреля 2015г.

ИНСТРУКЦИЯ
по организации парольной защиты доступа к информационным ресурсам, содержащим персональные данные МДОУ ДСКВ № 32 г.Ейска МО Ейский район

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаление учетных записей пользователей) доступа к информационным ресурсам, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на ответственных сотрудников образовательной организации.

2. Личные пароли и имена входов на доступ к информационным ресурсам назначаются и распределяются централизованно. Пароли на доступ в информационные подсистемы распределяются централизованно либо выбираются пользователями подсистемы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 7 символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, общепринятые наименования или сокращения, например, «ЭВМ», «User» и т.д.);
- при смене пароля новое значение должно отличатся от предыдущих значений пароля;
- личный пароль и имя входа пользователь должен хранить в секрете;

Владельцы паролей и имен входов перед их получением должны заполнить типовую анкету и быть предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение пароля и имени входа в информационную подсистему.

3. В случае если формирование личных паролей имен входов осуществляется централизованно, ответственность за правильность их

формирования и распределения возлагается на ответственных сотрудников образовательной организации.

4. Внеплановая смена личного пароля или удаление учетной записи пользователя информационной подсистемы в случае прекращения его полномочий (увольнения, переход на другую работу внутри организации и т.п.) должна производиться администраторами после окончания последнего сеанса работы данного пользователя соответствующей подсистемой.

5. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации) администратора, которому по роду работы были предоставлены полномочия по управлению парольной защитой доступа к информационной подсистеме.

6. В случае компрометации личного пароля пользователя информационной подсистемы, должны быть немедленно предприняты меры в соответствии с п.5 настоящей инструкции в зависимости от полномочий владельца скомпрометированного пароля.

7. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на ответственного сотрудника образовательной организации.

Ознакомлен:

_____Ведяева Е.М._____

(дата) (подпись) (Ф.И.О.)