Утверждено:
Директор
МБОУ СОШ № 8 им.А.Демина
_____ И.П.Лысенко
приказ от «06» 03 20 17 г.
№ 63

План работ МБОУ СОШ № 8 им.А.Демина по защите информации

Вводная часть

Целью работ по защите информации является предотвращение ущерба в результате ее разглашения, утраты, утечки, искажения, уничтожения и незаконного использования.

Объектами защиты являются:

- информационные ресурсы;
- средства и системы обработки информации;
- средства и системы защиты информации, в т.ч. криптографической защиты информации;
- помещения или объекты, предназначенные для ведения закрытых переговоров.

Основными источниками угроз безопасности информации являются:

- Стихийные – стихийные бедствия, катаклизмы;
- Техногенные: аварии, сбои и отказы оборудования;
- Ошибки эксплуатации;
- Преднамеренные действия нарушителей и злоумышленников.

Все нарушители делятся на две основные группы: внутренние и внешние. Предполагается, что несанкционированный доступ на объекты организации посторонних лиц исключается организационными мерами (охрана территории, организация пропускного режима).

Проведение работ по защите информации без финансовых затрат предполагает выработку организационно-режимных мероприятий, документации, проведение периодических контрольных мероприятий, поддержание системы в работоспособном и актуальном состоянии.

Требуется разработка следующих организационно-методических документов (примерный перечень):

- Концепция информационной безопасности МБОУ СОШ №8 им.А.Демина.
- Базовая модель угроз информационной безопасности.
- Перечень информационных ресурсов, подлежащих защите, с назначением ответственных за ресурс.
- Перечень защищаемых помещений.
- План защиты автоматизированных систем в МБОУ СОШ № 8 им.А.Демина.

- Положение о разграничении прав доступа к информационным ресурсам.
- Положение об использовании программного обеспечения.
- Положение об использовании сети Internet и электронной почты.
- Положение о парольной защите.
- Положение о резервном копировании.
- Положение об антивирусном контроле.
- Положение об использовании съемных носителях информации.
- Положение об использовании переносных компьютеров.
- Приказы о назначении ответственных лиц за антивирусный контроль, резервное копирование, предоставление доступа.
- Должностные инструкции ответственных по п.11.
- Памятка по защите информации для каждого сотрудника.
- Пакет документов по защите ПДн.
- Положение о порядке доступа к конфиденциальной информации МБОУ СОШ № 8 им.А.Демина.

Требуется провести следующие организационно-режимные мероприятия:

- Составить поэтажные планы размещения персональных компьютеров, серверов, средств коммутации и связи, локальной вычислительной сети, системы видеонаблюдения с целью выявления недостатков в области защиты.
- Ограничить доступ в серверную посторонних лиц, определив круг лиц, которые могут там находится и установив кодовый замок на помещение.
- Определить порядок именования рабочих станций и учетных записей пользователей, привязав их к расположению рабочей станции.
- Изменить тип учетных записей пользователей, понизив их с Администратора до Пользователя, в крайнем случае, до Опытного пользователя.
- Разграничить доступ к общим ресурсам на сервере на основе структуры организации, то есть свободный доступ к информации подразделения имеют лишь работники этого подразделения, а доступ работников других подразделений возможен только с согласия руководителя защищаемого подразделения.
- Изменить принцип организации парольной защиты – изменить тип пароля на сменяемый каждые 30 дней, возложить ответственность за сохранность секретности пароля на пользователя.
- Использование USB – устройств (флешки, съемные диски, USB-модемы) и записываемых CD, DVD как самого вероятного способа вирусного заражения и хищения конфиденциальной информации следует ограничить до минимально необходимого уровня.
- Ограничить доступ к развлекательным сайтам сети Internet.
- Расположить мониторы и печатающие устройства таким образом, чтобы исключить несанкционированный доступ к отображаемой и печатаемой информации.

- Блокировать рабочую станцию при временном отсутствии на рабочем месте.

По мере составления организационно-методических документов по защите информации потребуется проведение дополнительных организационно-режимных мероприятий.