Муниципальное общеобразовательное учреждение
средняя общеобразовательная школа №2
пгт.Новокручининский

Логинова Наталья Сергеевна
C=RU, O=МОУ СОШ 2 пгт.Новокручининский, CN=Логинова Наталья Сергеевна, E=nvkruchininskijj@mail.ru
I have reviewed this document
пгт. Новокручининский
2023-12-03 15:24:39

«Утверждаю»
Директор МОУ СОШ №2
пгт.Новокручининский
_____ Н.С.Логинова
Приказ № 94 от 03.11.2023г

Положение
об информационной безопасности
в МОУ СОШ №2 пгт.Новокручининский

1. Общие положения

1.1. Положение об информационной безопасности в МОУ СОШ №2 пгт.Новокручининский (далее - Положение) разработано в соответствии с Федеральным законом № 273-ФЭ от 29.12.2012 г. «Об образовании в Российской Федерации», Федеральным законом № 152- ФЗ от 27.07.2006 г. «О персональных данных», Федеральным законом Российской Федерации от 27.07.2006 года N 149-ФЗ «Об информации, информационных технологиях и о защите информации», Письмом Федерального агентства по образованию от 29.07.2009 г. № 17-110 «Об обеспечении защиты персональных данных». Письмом Министерства образования и науки РФ от 13.08.2002 г. N 01- 51-088ин «Об организации использования информационных и коммуникационных ресурсов в общеобразовательных учреждениях», Постановлением Правительства Российской Федерации от 17.11.2007 г. N 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. В понятие информационной безопасности образовательного учреждения входит система мер, направленная на защиту информационного пространства и персональных данных от случайного или намеренного проникновения с целью хищения каких-либо данных или внесения изменений в конфигурацию системы, защита образовательного процесса от любых сведений, носящих характер запрещенной законом пропаганды, или любых видов рекламы.

1.3. В составе массивов охраняемой законом информации, находящейся в распоряжении образовательного учреждения, можно выделить три группы:

- персональные сведения, касающиеся учащихся и преподавателей, оцифрованные архивы;
- структурированная учебная информация, обеспечивающая образовательный процесс (библиотеки, базы данных, обучающие программы).

1.4. Обязанностями лиц, ответственных за защиту информации, должно стать сохранение данных в целостности и неприкосновенности и обеспечение их:

- доступности в любое время для любого авторизированного пользователя;
- защиты от любой утраты или внесения несанкционированных изменений;
- конфиденциальности, недоступности для третьих лиц.

1. Угрозы информационной безопасности

1.1. Особенностью угроз становится не только возможность хищения сведений или повреждение массивов какими-либо сознательно действующими хакерскими группировками, но и сама деятельность подростков, намеренно, по злому умыслу или ошибочно способных повредить компьютерное оборудование или внести вирус.

1.2. Группы объектов, которые могут подвергнуться намеренному или ненамеренному воздействию:

• компьютерная техника и другие аппаратные средства, которые могут быть повреждены в результате механического воздействия, вирусов, по иным причинам;

• программы, используемые для обеспечения работоспособности системы или в образовательном процессе, которые могут пострадать от вирусов или хакерских атак;

• данные, хранимые как на жестких дисках, так и на отдельных носителях;

• сам персонал, отвечающий за работоспособность IT-систем;

• дети, подверженные внешнему агрессивному информационному влиянию и способные создать в школе криминальную ситуацию.

1.3. Угрозы, направленные на повреждение любого из компонентов системы, не зависящие от намерения персонала, учащихся или третьих лиц:

• любые аварийные ситуации, например, отключение электроэнергии или затопление;

• ошибки персонала;

• сбои в работе программного обеспечения;

• выход техники из строя;

• проблемы в работе систем связи.

2. Способы несанкционированного доступа

2.1. Человеческий. Информация может быть похищена путем копирования на временные носители, переправлена по электронной почте. При наличии доступа к серверу изменения в базы данных могут быть внесены вручную.

2.2. Программный. Для хищений сведений используются специальные программы, которые обеспечивают копирование паролей, копирование и перехват информации, перенаправление трафика, дешифровку, внесение изменений в работу иных программ.

2.3. Аппаратный способ связан или с использованием специальных технических средств, или с перехватом электромагнитного излучения по различным каналам, включая телефонные.

3. О системном администрировании и обязанностях ответственного за информационную безопасность

4.1 Задачи связанные с мерами системного администрирования, обеспечивающего информационную безопасность являются частью работы ответственного за информационную безопасность по обслуживанию компьютерной техники Учреждении.

4.2 Для решения задач информационной безопасности ответственный за информационную безопасность должен:

4.2.1 Следить за соблюдением требований по парольной защите, в том числе осуществлять изменение паролей по мере необходимости (утрата пароля, появление новых пользователей в связи с изменением кадрового состава и пр.)

4.2.2 Обеспечивать функционирование программно-аппаратного комплекса защиты по внешним цифровым линиям связи.

4.2.3 Обеспечивать мероприятия по антивирусной защите, как на уровне серверов, так и на уровне пользователей.

4.2.4 Обеспечивать нормальное функционирование системы резервного копирования.

4. Базы данных

4.1. Базы данных подлежащие защите вносятся в «Реестр баз данных подлежащих информационной защите».

4.2. Все процедуры по использованию и обслуживанию базы данных осуществляет ответственный за ведение базы данных. В том числе:

• резервное копирование;

• периодический контроль исправности резервных копий;

• подключение и отключение пользователей;

4.3. В случае если база данных требует парольной защиты, то ответственный за базу данных руководствуется требованиями раздела 6 «Система аутентификации» настоящего документа.

5. Система аутентификации

5.1. На всех ПК используется WINDOWS XP PROFESSIONAL, WINDOWS 7, WINDOWS 8.

5.2. Для использования локальной вычислительной сети в учебном процессе используются групповая идентификация: пользователь-ученик, пользователь учитель, администратор с разграничением прав доступа к папкам файлового сервера.

5.3. Для всех пользователей баз данных устанавливаются уникальные пароли. 6.4. Периодичность плановой смены паролей 1 раз в начале учебного года. 6.5. Установить блокировку учетной записи пользователей при неправильном наборе пароля более пяти раз.

6.6. Установить блокировку экрана и клавиатуры при отсутствии активности пользователя на рабочем месте более 30 мин., с последующим вводом пароля для разблокирования ПК.

6.7. Обязать пользователей осуществлять выход из базы данных, если планируется отсутствие на рабочем месте более 1,5 часов.

6.8. Обязать пользователей не разглашать сетевые реквизиты (имена и пароли) для доступа к информационным ресурсам, а также хранить их в недоступном месте.

6.9. Обслуживание системы аутентификации осуществляют ответственные за базы данных.

6. Защита по внешним цифровым линиям связи

6.1. В целях уменьшения риска повреждения программного обеспечения и утери информации, доступ из внутренней сети во внешнюю (Интернет, электронная почта) осуществляется через компьютеры с установленными брэндмауэром и антивирусом.

6.2. Запрещено несанкционированное использование модемов или иных средств доступа с ПК, подключенных к внутренней сети, во внешние сети.

6.3. Подключение школьных рабочих станций к внешним линиям связи

производится в локальной вычислительной сети по протоколам Ethernet и WiFi.

6.4. Запрещено подключение различных мобильных устройств (личных телефонов, планшетов и других гатжетов) к школьной сети WiFi.

7. Защита от несанкционированного подключения и размещение активного сетевого оборудования

7.1. Школьный\е сервер\а размещаются в кабинете информатики при отсутствии специально выделенной серверной.

7.2. Доступ к серверу ограничен паролем, который известен только ответственному за информационную безопасность, ответственному за информатизацию.

7.3. Роутеры, точки доступа и прочее активное сетевое оборудование должно располагаться в местах по возможности исключающих свободный доступ.

8. Процедура увольнения сотрудников имеющих доступ к сети

8.1. В случае кадровых перестановок и изменений все ответственные за базы данных переназначаются приказом директора, новым сотрудникам предоставляются логины и пароли для доступа к базам данных.

9. Антивирусная защита

9.1.На основании Правил пользования внешними сетевыми ресурсами (Интернет, электронная почта и т.д.) не допускается работа без организации антивирусной защиты. Антивирусная защита организуется на уровне рабочих станций и сервера посредством лицензионного антивирусного программного обеспечения.

9.2. Обновление базы используемого антивирусного программного обеспечения осуществляется автоматически не реже 1 раза в день.

9.3. За своевременное обновление антивирусного программного обеспечения отвечает ответственный за информационную безопасность.