Муниципальное общеобразовательное учреждение
средняя общеобразовательная школа № 3

Согласовано:
Инженер ИТ
Г.С. Махнев

Утверждаю:
Директор МОУ СОШ № 3
Н.В. Серебренникова
«07» апреля 2014 г.

Положение по информационной безопасности МОУ СОШ №3

1. Общие положения

1.1 МОУ СОШ №3 – объект, на котором развернута локально-вычислительная сеть, подлежащая информационной защите.

1.2 Под безопасностью локально-вычислительной сети МОУ СОШ №3 понимается ее защищенность от случайного или преднамеренного вмешательства в нормальный процесс функционирования, а также от попыток хищения, модификации или разрушения ее компонентов. Безопасность системы достигается обеспечением конфиденциальности обрабатываемой ею информации, а также целостности и доступности компонентов и ресурсов системы.

1.3 *Конфиденциальность компьютерной информации* — это свойство информации быть известной только допущенным и прошедшим проверку (авторизацию) субъектам системы (пользователям, программам, процессам и т. д.).

Целостность компонента (ресурса) системы — свойство компонента (ресурса) быть неизменным (в семантическом смысле) при функционировании системы.

Доступность компонента (ресурса) системы — свойство компонента (ресурса) быть доступным для использования авторизованными субъектами системы в любое время.

Доступ детей к информации - возможность получения и использования детьми свободно распространяемой информации.

Зрелищное мероприятие - демонстрация информационной продукции в месте, доступном для детей, и в месте, где присутствует значительное число лиц, не принадлежащих к обычному кругу семьи, в том числе посредством проведения театрально-зрелищных, культурно-просветительных и зрелищно-развлекательных мероприятий.

Информационная безопасность детей - состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

Информационная продукция - предназначенные для оборота на территории Российской Федерации продукция средств массовой информации, печатная продукция, аудиовизуальная продукция на любых видах носителей, программы

для электронных вычислительных машин (программы для ЭВМ) и базы данных, а также информация, распространяемая посредством зрелищных мероприятий, посредством информационно-телекоммуникационных сетей, в том числе сети "Интернет", и сетей подвижной радиотелефонной связи.

информация, причиняющая вред здоровью и (или) развитию детей, - информация (в том числе содержащаяся в информационной продукции для детей), распространение которой среди детей запрещено или ограничено в соответствии с Федеральным законом от 29 декабря 2010 г. № 436-ФЗ.

Места, доступные для детей, - общественные места, доступ ребенка в которые и (или) нахождение ребенка в которых не запрещены, в том числе общественные места, в которых ребенок имеет доступ к продукции средств массовой информации и (или) размещаемой в информационно-телекоммуникационных сетях информационной продукции.

Оборот информационной продукции - предоставление и (или) распространение информационной продукции, включая ее продажу (в том числе распространение по подписке), аренду, прокат, раздачу, выдачу из фондов общедоступных библиотек, публичный показ, публичное исполнение (в том числе посредством зрелищных мероприятий), распространение посредством эфирного или кабельного вещания, информационно-телекоммуникационных сетей, в том числе сети "Интернет", и сетей подвижной радиотелефонной связи.

1.4 Безопасность системы обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств, программ, данных и служб с целью обеспечения доступности, целостности и конфиденциальности связанных с компьютерами ресурсов; сюда же относятся и процедуры проверки выполнения системой определенных функций в строгом соответствии с их запланированным порядком работы.

1.5 Систему обеспечения безопасности можно разбить на следующие подсистемы:

- ✓ компьютерную безопасность;
- ✓ безопасность данных;
- ✓ безопасное программное обеспечение;
- ✓ безопасность коммуникаций.

Компьютерная безопасность обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств компьютера с целью обеспечения доступности, целостности и конфиденциальности связанных с ним ресурсов.

Безопасность данных достигается защитой данных от неавторизованных, случайных, умышленных или возникших по халатности модификаций, разрушений или разглашения.

Безопасное программное обеспечение представляет собой общецелевые и прикладные программы и средства, осуществляющие безопасную обработку данных в системе и безопасно использующие ресурсы системы.

Безопасность коммуникаций обеспечивается посредством аутентификации телекоммуникаций за счет принятия мер по предотвращению предоставления неавторизованным лицам критичной информации, которая может быть выдана системой в ответ на телекоммуникационный запрос.

1.6 К объектам информационной безопасности МОУ СОШ №3 относят:

- информационные ресурсы, содержащие сведения, отнесенные к коммерческой тайне, и конфиденциальную информацию, представленную в виде документированных информационных массивов и баз данных;
- средства и системы информатизации — средства вычислительной и организационной техники, сети и системы, общесистемное и прикладное программное обеспечение, автоматизированные системы управления рабочими местами, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации, а также их информативные физические поля.

2. Положение о инженере ИТ

2.1 Задачи связанные с информационной безопасностью являются прерогативой инженера ИТ.

2.2 Для решения задач информационной безопасности инженер ИТ должен:

2.2.1 Следить за соблюдением требований по парольной защите, в том числе осуществлять изменение паролей согласно п. 4.3;

2.2.2 Обеспечивать функционирование программно-аппаратного комплекса защиты по внешним цифровым линиям связи;

2.2.3 Обеспечивать мероприятия по антивирусной защите, как на уровне серверов, так и на уровне пользователей;

2.2.4 Обеспечивать нормальное функционирование системы резервного копирования.

3. Базы данных

3.1 Для каждой базы данных приказом директора МОУ СОШ №3 должен назначаться Администратор базы данных.

3.2 Все процедуры по использованию и обслуживанию базы данных осуществляет Администратор базы данных. В том числе:

- резервное копирование;
- периодический контроль исправности резервных копий;
- подключение и отключение пользователей;
- внесение изменений в структуру базы
- прочие виды работ связанных с данной базой.

3.3 В случае если база данных требует парольной защиты, то Администратор базы руководствуется требованиями главы 4 настоящего документа «Система аутентификации», в которой описаны требования к паролям, их длине, месту хранения, и т.д.

4. Система аутентификации

4.1 На всех клиентских ПК использовать операционную систему согласно приобретенным лицензиям.

4.2 Для всех пользователей устанавливать уникальные пароли длиной не менее 8 знаков.

4.3 Периодичность плановой смены паролей 2 раз в год.

4.4 Установить блокировку учетной записи пользователей при неправильном наборе пароля более пяти раз.

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

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

4.7 Обслуживание системы аутентификации осуществляет инженер ИТ.

4.8 Базу пользовательских паролей хранить на машинных носителях только в зашифрованном виде.

4.9 Пароли администраторов хранить в запечатанных конвертах, в местах исключающих свободный доступ.

5. Защита по внешним цифровым линиям связи

5.1 В целях уменьшения риска повреждения программного обеспечения и утери информации, доступ из внутренней сети во внешнюю (Интернет, электронная почта) осуществляется через одну точку защищенную от несанкционированного доступа извне брандмауэром и антивирусом.

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

5.3 Время доступа и тип программного обеспечения, посредством которого осуществляется доступ во внешние сети определяется инженером ИТ.

6. Защита от несанкционированного подключения к ЛВС и размещение активного сетевого оборудования

6.1 Для размещения серверов оборудуются специальные серверные комнаты, имеющие два независимых ввода по питанию (~220В), источники бесперебойного питания, систему кондиционирования и оборудованные пожарной и охранной сигнализацией.

6.2 В серверных комнатах не допускается оборудование постоянных рабочих мест для персонала.

6.3 В случае необходимости выполнения каких-либо работ в серверных комнатах посторонним персоналом (электрики, сантехники, уборщики и т.д.) обязательно присутствие наблюдающего из группы АСУ (инженер ИТ или его заместители).

6.4 Коммутаторы, концентраторы и прочее активное сетевое оборудование должно располагаться в местах исключающих свободный доступ.

7. Договор с пользователями о неразглашении

При заключении трудового договора с сотрудниками специально оговаривается ответственность сотрудника на случай разглашения им информации связанной с функционированием ЛВС МОУ СОШ №3. К такой информации относятся имена пользователей, пароли, архитектура сети, виды применяемых методов защиты и т.д. При получении доступа к сетевым ресурсам, пользователи должны проходить вводный инструктаж с регистрацией в специальном журнале и получать на руки памятку (составленную на базе «Положения по информационной безопасности»), содержащую перечень

требований по информационной безопасности обязательных для выполнения. Ответственный за инструктаж – инженер по ОТиТБ.

8. Процедура увольнения сотрудников имеющих доступ к сети

8.1 В случае увольнения инженера ИТ, или администратора какого-либо уровня (администратор базы данных, менеджер группы и т.д.), после подписания заявления об увольнении немедленно назначается исполняющий обязанности увольняемого сотрудника, который меняет все пароли доступа к ресурсам подконтрольным увольняемому сотруднику. На учетную запись увольняемого администратора устанавливается ограничение по дате с учетом даты фактического прекращения работы увольняемого.

8.2 В случае увольнения рядового пользователя, после подписания заявления об увольнении руководитель структурного подразделения уведомляет служебной запиской инженера ИТ о дате фактического прекращения работы увольняемого пользователя. Инженер ИТ устанавливает ограничения по дате на учетную запись увольняемого сотрудника, по истечении которой учетная запись будет заблокирована, а в дальнейшем уничтожена. Новый сотрудник, принимаемый в последствии на данное рабочее место должен получать НОВУЮ учетную запись, с НОВЫМ именем и паролем.

9. Правила пользования внешними сетевыми ресурсами (Интернет, электронная почта и т.д.).

Основным способом проникновения компьютерных вирусов на компьютер пользователя в настоящее время является Интернет и электронная почта. В связи с этим не допускается работа без организации антивирусной защиты, которая располагается на каждом персональном компьютере. При необходимости возможна установка дополнительной антивирусной защиты на шлюзовом оборудовании. Тип применяемого антивирусного программного обеспечения определяется инженером ИТ и является общим для всего МОУ СОШ №3. Обновление базы используемого антивирусного программного обеспечения осуществляется автоматически не реже 1 раза в неделю. Своевременность обновления антивирусного программного обеспечения обеспечивает инженер ИТ.

10. Защита детей от информации, причиняющей вред их здоровью и развитию

10.1 Согласно части 2 статьи 11 Федерального закона Российской Федерации от 29 декабря 2010 г. № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" оборот информационной продукции, содержащей информацию, запрещенную для распространения среди детей, в местах, доступных для детей, не допускается без применения административных и организационных мер, технических и программно-аппаратных средств защиты детей от указанной информации.

10.2 Доступ к информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети "Интернет" для детей предоставляется только в компьютерных классах, при условии применения административных и организационных мер, технических, программно-

аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию. Доступ предоставляется только в присутствии ответственного преподавателя и только после проверки преподавателем надлежащего функционирования технических, программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию.

10.3 Допуск детей к вычислительной технике на которой не установлены программно-аппаратные средства защиты не допустим!

10.4 Ответственность за функционирование программно-аппаратных средств защиты несет инженер ИТ.

10.5 До начала демонстрации посредством зрелищного мероприятия информационной продукции ей присваивается знак информационной продукции. В случае демонстрации нескольких видов информационной продукции для детей разных возрастных категорий указанный знак должен соответствовать информационной продукции для детей старшей возрастной категории. Указанный знак размещается на афишах и иных объявлениях о проведении зрелищного мероприятия, а также на входных билетах, приглашениях и иных документах, предоставляющих право его посещения.

10.6 Демонстрация посредством зрелищного мероприятия информационной продукции, содержащей информацию, предусмотренную статьей 5 Федерального закона от 29 декабря 2010 г. № 436-ФЗ (информация, причиняющая вред здоровью и (или) развитию детей), предваряется непосредственно перед началом зрелищного мероприятия звуковым сообщением о недопустимости или об ограничении присутствия на такой демонстрации детей соответствующих возрастных категорий.

11. Использование средствам криптографической защиты информации

11.1 При установке криптосредств (ключей шифрования) на ПК приказом ограничивается круг лиц, допущенных к использованию ПК.

11.2 Допуск к ПК с установленными средствами криптографической защиты посторонних лиц, а равно лиц, не допущенных приказом запрещается!

11.3 При нарушении требований п. 11.2 работник привлекается к дисциплинарной ответственности согласно ТК РФ, а также к другой ответственности, предусмотренной законодательством РФ.

11.4 При установке криптосредств на ПК, пользователю, допущенному к работе с ними, выдается памятка по информационной безопасности (приложение 1).

Приложение 1

ПАМЯТКА

Пользователю криптосредств

1. Не разглашать следующие сведения:

– применяемых криптосредствах и других средствах защиты (название, версия и т.д.);
– порядке функционирования криптосредств, в том чиле ошибок в работе, функционале, настройках, закономерностях, выявленных в процессе работы;
– порядке охраны помещений, компьютеров, составе и настройке других средств защиты, например антивирусных программ;
–пароль и парольную фразу от криптосредства, учетной записи операционной системы, которые запрашиваются при включении компьютера и входе в систему.

2. Не хранить пароли и парольные фразы в электронном виде.

3. Не передавать и не сообщать пароль никому, даже администраторам. При необходимости – ввести пароль лично. При попытке выяснить пароль немедленно сообщать ответственному.

4. Не передавать другим пользователям пароли, ключи шифрования, установленных на компьютере криптосредств. О необходимости такой передачи необходимо уведомить ответственного.

5. Обязательно блокировать рабочий стол компьютера при отсутствии на рабочем месте.

6. Если пароль стал известен посторонним лицам, или другим пользователям – сменить пароль (длина пароля не менее 9 символов). Если пользователи, или посторонние лица могли иметь доступ к компьютеру – сообщить ответственному.

7. Заходить на компьютер только со своим паролем, под своей учетной записью. Не заходить под учетной записью других пользователей, с использованием их паролей.

8. До включения компьютера необходимо проверить целостность пломб и индикаторных наклеек, которыми опечатаны системные блоки. В случае нарушения целостности – не включать компьютер и сообщить ответственному. Наклейки и пломбы не срывать!!!

9. В кабинете не должны бесконтрольно находиться посторонние лица, в том числе при уборке помещения. Не оставлять пустой кабинет открытым, необходимо закрыть его на ключ.

10. Не передавать ключи от помещений посторонним лицам. Помещение вскрывается только сотрудниками, осуществляющими в них свои трудовые обязанности, или ответственным.

11. Не допускать посторонних лиц к своим рабочим местам и компьютерам. Не допускать непреднамеренного удаления средств защиты, ключей шифрования.

12. При попытке посторонних лиц узнать сведения о защищаемых персональных данных, сведениях из пункта 1 – сообщить ответственному.

13. В конце рабочего дня закрыть помещение на ключ, ключи передать на пост охраны.

14. Если помещение вскрыто, необходимо незамедлительно оповестить ответственного и пост охраны.

15. Сообщать ответственному о нарушениях инструкции и памятки, которые могут привести к раскрытию паролей, персональных данных.

16. При утрате или недостаче ключей от помещений, хранилищ, личных печатей – сообщить ответственному.

17. При неисправности компьютера, ошибках в работе программ – сообщить в службу техподдержки.

Приложение 2

ПАМЯТКА ПОЛЬЗОВАТЕЛЯ ПК

1. Не разглашать следующие сведения:

   – применяемых криптосредствах и других средствах защиты (название, версия и т.д.);
   – порядке функционирования криптосредств, в том чиле ошибок в работе, функционале, настройках, закономерностях, выявленных в процессе работы;
   – порядке охраны помещений, компьютеров, составе и настройке других средств защиты, например антивирусных программ;
   –пароль и парольную фразу от криптосредства, учетной записи операционной системы, которые запрашиваются при включении компьютера и входе в систему.

2. Не хранить пароли и парольные фразы в электронном виде.

3. Не передавать и не сообщать пароль никому, даже администраторам. При необходимости – ввести пароль лично. При попытке выяснить пароль немедленно сообщать ответственному.

4. Обязательно блокировать рабочий стол компьютера при отсутствии на рабочем месте.

5. Если пароль стал известен посторонним лицам, или другим пользователям – сменить пароль (длина пароля не менее 8 символов).

6. Заходить на компьютер только со своим паролем, под своей учетной записью. Не заходить под учетной записью других пользователей, с использованием их паролей. Не допускать использования ПК доступ к которым ограничен.

7. До включения компьютера необходимо проверить целостность пломб и индикаторных наклеек, которыми опечатаны системные блоки. В случае нарушения целостности – не включать компьютер и сообщить ответственному. Наклейки и пломбы не срывать!!!

8. Не передавать ключи от помещений посторонним лицам. Помещение вскрывается только сотрудниками, осуществляющими в них свои трудовые обязанности, или ответственным.

9. Не допускать посторонних лиц к своим рабочим местам и компьютерам. Не допускать непреднамеренного удаления средств защиты, ключей шифрования.

10. При попытке посторонних лиц узнать сведения о защищаемых персональных данных, сведениях из пункта 1 – сообщить ответственному.

11. Сообщать ответственному о нарушениях инструкции и памятки, которые могут привести к раскрытию паролей, персональных данных.

12. При неисправности компьютера, ошибках в работе программ – сообщить в службу техподдержки.