Рассмотрено и принято
на педагогическом совете
протокол № **1** от **15.08.2015**

Утверждено
Приказ № 51 от 15.08. 2015

Директор школы А.Ю. Чудагашев

**ПОЛОЖЕНИЕ**
**по информационной безопасности**
**МБОУ-Барышевская СОШ № 9**

1. Общие положения

Данный локальный акт регламентирует вопросы информационной безопасности в Муниципальном бюджетном образовательном учреждении Новосибирского района Новосибирской области – Барышевская средняя общеобразовательная школа№9 ( МБОУ-Барышевская СОШ № 9).

В МБОУ- Барышевская СОШ № 9 развернута локально-вычислительная сеть с выходом в интернет, подлежащая информационной защите.

Под безопасностью локально-вычислительной сети МБОУ-Барышевская СОШ № 9 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.

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.

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.

К объектам информационной безопасности МБОУ-БарышевскаяСОШ № 9 относят:

-информационные ресурсы, содержащие конфиденциальную информацию, представленную в виде документированных информационных массивов и баз данных;

- средства и системы информатизации — средства вычислительной и организационной техники, локальной сети, общесистемное и прикладное программное обеспечение, автоматизированные

системы управления рабочими местами, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации.
2. О системном администрировании и обязанностях ответственного за информационную безопасность
2.1 Задачи связанные с мерами системного администрирования, обеспечивающего информационную безопасность являются частью работы ответственного за информационную безопасность по обслуживанию компьютерной техники в МБОУ-Барышевская СОШ № 9.
2.2 Для решения задач информационной безопасности ответственный за информационную безопасность должен:
2.2.1 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.);
2.2.2 Обеспечивать функционирование программно-аппартного 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. Система аутентификации
3.1. На всех клиентских ПК используется WINDOWS XP PROFESSIONAL, WINDOWS 7, WINDOWS 8, Red Hat Enterprise Linux 6 (LinuxWizard).
3.2. Для использования локальной вычислительной сети в учебном процессе используются групповая идентификация: пользователь-ученик, пользователь учитель, администратор с разграничением прав доступа к папкам файлового сервера.
3.3. Для всех пользователей баз данных устанавливаются уникальные пароли.
3.3. Периодичность плановой смены паролей 1 раз в начале учебного года.
3.4. Установить блокировку учетной записи пользователей при неправильном наборе пароля более пяти раз.
3.5. Установить блокировку экрана и клавиатуры при отсутствии активности пользователя на рабочем месте более 30 мин., с последующим вводом пароля для разблокирования ПК.
3.6. Обязать пользователей не разглашать сетевые реквизиты (имена и пароли) для доступа к информационным ресурсам, а также хранить их в недоступном месте.
3.7. Обслуживание системы аутентификации осуществляет ответственный за информационную безопасность.
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 компьютеры с установленными брэндмауэром и антивирусом.
5.2. Запрещено несанкционированное использование модемов или иных средств доступа с ПК, подключенных к внутренней сети, во внешние сети.
5.3. Подключение школьных рабочих станций к внешним линиям связи производится в локальной вычислительной сети по протоколам Ethernet.
5.4. Запрещено подключение различных мобильных устройств (личных телефонов, планшетов и других гатжетов) к школьной сети WiFi.
6. Защита от несанкционированного подключения к ЛВС и размещение активного сетевого оборудования
6.1. Школьный\е сервер\а размещаются в кабинете информатики при отсутствии специально выделенной серверной.
6.2. Доступ к серверу ограничен паролем, который известен только ответственному за информационную безопасность.
6.3. Коммутаторы, концентраторы, роутеры, точки доступа и прочее активное сетевое оборудование должно располагаться в местах по возможности исключающих свободный доступ.

7. Процедура увольнения сотрудников имеющих доступ к сети

7.1 В случае кадровых перестановок и изменений все ответственные за информационную безопасность переназначаются приказом директора, новым сотрудникам предоставляются логины и пароли для доступа.

8. Антивирусная защита

8.1. 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. Антивирусная защита организуется на уровне рабочих станций и сервера посредством лицензионного антивирусного программного обеспечения.

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

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