МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«КУБАНСКАЯ ШКОЛА»
297541, Республика Крым, Симферопольский р-н, п. Школьное, ул.Мира, дом 32
тел. (0652) 55-20-87, e-mail: kybanskaya1961@mail.ru

СОГЛАСОВАНО
Председатель профкома
_____С.А.Вержак

УТВЕРЖДЕНО
Приказом от 25.02.16 № 39/од
Директор МБОУ «Кубанская школа»
_____Н.В. Скуратовская

ПОЛОЖЕНИЕ № 57
ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МУНИЦИПАЛЬНОМ БЮДЖЕТНОМ ОБЩЕОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ «КУБАНСКАЯ ШКОЛА»

1.Общие положения

1.1.Настоящее Положение регулирует вопросы информационной безопасности в Муниципальном бюджетном общеобразовательном учреждении «Кубанская школа».

1.2. Под информационной безопасностью 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.

Систему обеспечения безопасности можно разбить на следующие подсистемы:

1) компьютерную безопасность;
2) безопасность персональных данных;
3) безопасное программное обеспечение;
4) 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. 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 «Кубанская школа» относят:

1) информационные ресурсы, содержащие конфиденциальную информацию, представленную в виде документированных информационных массивов и баз данных;
2) 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. Обязанности и права должностных лиц

2.1. Директор организует работу по построению системы защиты информационной системы. В частности:

1) назначает ответственного, за организацию защиты информации из числа сотрудников школы;
2) утверждает состав комиссии по организации работ по защите информации;
3) утверждает комплект документов, определяющих политику в отношении обработки персональных данных в общеобразовательном учреждении; локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации.

2.2. Заместитель директора по безопасности:

1) участвует в разработке локальных и нормативных актов;
2) контролирует работу ответственного за информационную безопасность образовательного учреждения;
3) контролирует порядок подготовки, учета и хранения документов конфиденциального характера;
4) организует выполнение мероприятий по защите информации при использовании технических средств;
5) участвует в определении мест установки и количества АРМ, необходимых для обработки информации.

2.3.Ответственный за информационную безопасность должен:

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) обеспечивать функционирование программно-аппаратного комплекса защиты по внешним цифровым линиям связи;
3) обеспечивать мероприятия по антивирусной защите, как на уровне серверов, так и на уровне пользователей;
4) обеспечивать нормальное функционирование системы резервного копирования.

3. Система аутентификации

3.1. На всех клиентских ПК используетсяWINDOWS 7.

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

3.3. Периодичность плановой смены паролей 1 раз в начале учебного года.

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

3.5.Обслуживание системы аутентификации осуществляет ответственный по информационной безопасности.

4. Защита по внешним цифровым линиям связи

4.1. В целях уменьшения риска повреждения программного обеспечения и утери информации, доступ из внутренней сети во внешнюю (Интернет, электронная почта) осуществляется через компьютеры с установленным антивирусом.
4.2. Запрещено несанкционированное использование модемов или иных средств доступа с ПК, подключенных к внутренней сети, во внешние сети.
4.3. Подключение школьных рабочих станций к внешним линиям связи производится в локальной вычислительной сети по протоколам Ethernet и WiFi.
4.4. Запрещено подключение различных мобильных устройств (личных телефонов, планшетов и других гатжетов) к школьной сети WiFi.

5. Защита от несанкционированного подключения и размещения активного сетевого оборудования

5.1. Школьный сервер размещается в кабинете информатики при отсутствии специально выделенной серверной.
5.2. Доступ к серверу ограничен паролем, который известен только ответственному за информационную безопасность, заместителю директора по безопасности, директору школы.
5.3. Роутеры, точки доступа и прочее активное сетевое оборудование должно располагаться в местах по возможности исключающих свободный доступ.

6. Антивирусная защита

6.1. 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.
6.2. Обновление базы используемого антивирусного программного обеспечения осуществляется автоматически не реже 1 раза в день.
6.3. За своевременное обновление антивирусного программного обеспечения отвечает ответственный за информационную безопасность.

Пронумеровано,
прошнуровано,
скреплено печатью
четыре
листа

Директор Н.В. Скуратовская