Муниципальное бюджетное общеобразовательное учреждение
«Майская средняя общеобразовательная школа»
(МБОУ «Майская СОШ»)

УТВЕРЖДЕНО:
Директор
_____ Р.Ю. Шульга
приказ № 123 от «3» 09 2018 г.

Положение
об информационной безопасности

I. Общие положения

1.1. Настоящее Положение об информационной безопасности (далее - Положение) регламентирует вопросы информационной безопасности Муниципального бюджетного общеобразовательного учреждения «Майская средняя общеобразовательная школа (далее - Учреждение).

1.2. Настоящее Положение определяется в соответствии с нормативными правовыми актами:
- Федеральным законом от 27.06.2007 г. № 152-ФЗ «О персональных данных»;
- Постановлением Правительства РФ от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена ФСТЭК 14.02.2008 г.).

1.3. Целью настоящего Положения является обеспечение необходимых мер для защиты информации, ресурсов и технических средств информационной системы от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в Учреждении.

1.4. Требования настоящего Положения распространяются на всю информацию и ресурсы обработки информации Учреждения.

1.5. Соблюдение настоящего Положения обязательно для всех работников (как постоянных, так и временных). Ответственность за соблюдение информационной безопасности несет каждый работник Учреждения.

1.6. В договорах с третьими лицами, получающими доступ к информации Учреждения, должна быть оговорена обязанность третьего лица по соблюдению требований настоящего Положения.

II. Основные понятия, используемые в настоящем положении

2.1. В настоящем Положении используются следующие основные понятия:
- **Автоматизированное рабочее место (АРМ)** - программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида;
- **Администратор информационной безопасности** - работник, должностные обязанности которого подразумевают обеспечение безопасности компьютерной техники, сети и программного обеспечения в организации;
- **Аутентификация** - процедура проверки подлинности пользователя информационной системы путём сравнения введённого им пароля с паролем сохранённым в базе данных пользователей;
- **База данных (БД)** - совокупность данных, организованная в соответствии с

определенными правилами и поддерживаемая в памяти компьютера;

- **Безопасность информации (данных)** - состояние защищённости информации (данных), при котором обеспечиваются её (их) конфиденциальность, доступность и целостность.
- **Информационная безопасность (ИБ)** - состояние защищенности данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность данных при их обработке в информационных системах данных;
- **Информационная система (ИС)** - система, предназначенная для хранения, поиска и обработки информации и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию;
- **Информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- **Доступ к информации** - возможность получения информации и её использования;
- **Доступ к информационной системе** - получение возможности ознакомления с информацией, её обработки и (или) воздействия на информацию и (или) ресурсы автоматизированной информационной системы с использованием программных и (или) технических средств;
- **Контролируемая зона** - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц;
- **Конфиденциальность информации** - это свойство информации быть известной только допущенным и прошедшим проверку (авторизацию) субъектам системы (пользователям, программам, процессам и т.д.);
- **Локальная вычислительная сеть (ЛВС)** - компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, школу);
- **Нарушитель безопасности** - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности данных при их обработке техническими средствами в информационных системах данных;
- **Носители данных** - материальные объекты или устройства с определёнными физическими свойствами, позволяющими использовать их для записи, хранения и считывания данных;
- **Операционная система (ОС)** - комплекс взаимосвязанных программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем;
- **Пользователь информационной системы** - лицо, участвующее в функционировании информационной системы данных или использующее результаты её функционирования;
- **Правила разграничения доступа** - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа;
- **Программное воздействие** - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ;
- **Программное обеспечение (ПО)** - все или часть программ, процедур, правил и соответствующей документации системы обработки информации;
- **Ресурс информационной системы** - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы;
- **Система контентной фильтрации (СКФ)** - устройство или программное обеспечение для фильтрации сайтов по их содержимому, не позволяющее получить

доступ к определённым сайтам или услугам сети Интернет, система позволяет блокировать веб-сайты с содержимым, не предназначенным для просмотра;

- **Технические средства информационной системы данных** - средства вычислительной техники, информационно-вычислительные комплексы и сети, программные средства (операционные системы, системы управления базами данных), средства защиты информации, применяемые в информационных системах;
- **Угрозы безопасности данных** - действия, в результате которых невозможно восстановить содержание данных в информационной системе данных или в результате которых уничтожаются материальные носители данных;
- **Уязвимость** - слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации;
- **Целостность информации (данных)** - состояние информации (данных), характеризующее, что данные не были изменены при выполнении какой-либо операции над ними, будь то передача, хранение или отображение.

III. Информационная система данных

3.1. Информационная система данных в Учреждении классифицируется:

3.1.1. По характеристике как типовая, в которой необходимо обеспечить конфиденциальность данных (защищенность от уничтожения, изменения, блокирования, а также несанкционированных действий).

3.1.2. По структуре - локальная, развернутая на контролируемой зоне в пределах одного здания, в котором исключено неконтролируемое пребывание посторонних лиц, нарушителей безопасности.

3.1.3. По наличию подключения к сетям связи общего пользования - имеющая подключение к локальной сети Интернет.

3.1.4. По режиму обработки данных в ИС - многопользовательский уровень.

3.1.5. По разграничению прав доступа пользователей - с разграничением прав доступа пользователей, допущенных к обработке данных.

IV. Информационная безопасность

4.1. Информационная безопасность системы достигается обеспечением конфиденциальности обрабатываемой ею информации, а также целостности и доступности компонентов и ресурсов ИС.

4.2. Под ИБ понимается её защищенность от угроз безопасности данных, то есть случайного или преднамеренного вмешательства в нормальный процесс её функционирования, а также действий, в результате которых невозможно восстановить содержание данных в ИС данных или в результате которых уничтожаются материальные носители данных.

4.3. Безопасность данных при их обработке в ИС обеспечивается с помощью системы обеспечения безопасности, включающей в себя комплекс организационных и технологических мер, применяемых в отношении технических средств ИС данных, ПО, определенных с учётом актуальных угроз безопасности данных.

4.4. Безопасность данных при их обработке в ИС обеспечивает лицо, осуществляющее обработку данных в БД.

4.5. При обнаружении уязвимости ИС пользователь ИС должен незамедлительно сообщить о данном инциденте администратору ИБ.

V. Система обеспечения безопасности

5.1. Систему обеспечения безопасности можно разбить на следующие подсистемы:

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

ресурсов:

- защиту от внешних несанкционированных воздействий (аппаратные и программные средства);
- контроль за электронной почтой (входящая и исходящая корреспонденция);
- контроль за информацией, циркулирующей в локальной сети;
- контроль за информацией, хранящейся на внешних носителях.

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

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

VI. Базы данных

6.1. Базы данных, организованные в соответствии с определенными правилами в Учреждении, обрабатываемые с использованием информационных технологий, подлежат защите и вносятся в «Реестр баз данных, подлежащих информационной защите» (Приложение №1).

6.2. Для каждой БД, включенной в «Реестр баз данных, подлежащих информационной защите» приказом руководителя Учреждения по предоставлению комиссии по ИБ назначается ответственное лицо за ведение БД.

6.3. Процедуры по использованию БД осуществляет ответственный за ведение базы данных, в том числе:

- внесение в структуру БД, а также изменении в «Реестр баз данных, подлежащих информационной защите», при необходимости (изменение степени конфиденциальности, места расположения и т.д.);
- внесение изменений в БД.

6.4. Процедуры по обслуживанию БД осуществляет администратор информационной безопасности, в том числе:

- хранение БД;
- копирование БД;
- прочие виды работ, связанные с БД.

VII. Система аутентификации

7.1. На всех персональных компьютерах используется Windows 7, Windows 8, Windows 10.

7.2. Обслуживание системы аутентификации осуществляет администратор информационной безопасности Учреждения.

7.3. Администратор информационной безопасности должен:

7.3.1. Осуществлять:

- антивирусную защиту ресурсов ИС с использованием лицензионного антивирусного ПО на всех АРМ Учреждения, а также своевременное обновление антивирусных баз (сигнатур и т.п.);
- программный комплекс мер СКФ ресурсов ИС;
- парольную защиту технических средств ИС;
- резервное копирование БД;
- периодический контроль исправности резервных копий.

7.3.2. Использовать для использования локальной сети в учебном процессе групповую идентификацию: «пользователь-ученик», «пользователь-учитель», «администратор».

7.3.3. Установить для всех пользователей БД уникальные пароли.

7.3.4. Осуществлять смену паролей с периодичностью не менее одного раза в год.

7.3.5. Установить блокировку учётной записи пользователей при неправильном наборе

пароля более 5 раз.

7.3.6. Установить блокировку экрана и клавиатуры при отсутствии активности пользователя на рабочем месте более 15 минут, с последующим вводом пароля для разблокирования персонального компьютера.

7.3.7. Вести журнал назначения и смены паролей единый для всех БД.

7.3.8. Обязать пользователей осуществлять выход из БД, если планируется отсутствие на рабочем месте более 1,5 часов.

VIII. Антивирусная зашита

8.1. Антивирусная защита предназначена для обеспечения защиты программного воздействия на АРМ пользователей ИС Учреждения с использованием вирусов и вредоносных программ.

8.2. На любом работающем компьютере при вводе в эксплуатацию или после переустановки операционной системы администратором ИБ в обязательном порядке устанавливается и активируется антивирусная программа.

8.3. Отключение или не обновление антивирусных средств не допускается.

8.4. Установка и обновление антивирусных средств в Учреждении контролируется администратором ИБ.

IX. Защита оборудования

9.1. Работники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранятся информация Учреждения.

9.2. Работникам запрещено самостоятельно изменять конфигурацию аппаратного и ПО.

X. Защита по внешним цифровым линиям связи

10.1. В целях уменьшения риска повреждения ПО и утери информации, доступ из внутренней сети во внешнюю (Интернет, электронная почта) осуществляется через компьютеры с установленным брэндмауэром, антивирусом).

10.2. Подключение компьютеров Учреждения к внешним линиям связи производится в ЛВС по протоколам INTERNET и WiFi.

10.3. Запрещено подключение различных мобильных устройств (личных телефонов, планшетов и других гаджетов) к ЛВС Учреждения.

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

XI. Контроль доступа к информационным системам

11.1. В целях обеспечения санкционированного доступа к ресурсу ИС, любой вход в систему должен осуществляться с использованием уникального имени пользователя (логина) и пароля.

11.2. Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим.

11.3. Доступ третьих лиц к ИС Учреждения должен быть обусловлен производственной необходимостью, в связи с этим, порядок доступа к ИС Учреждения должен быть четко определен, контролируем и защищен.

11.4. Каждый сотрудник обязан немедленно уведомить руководителя Учреждения и администратора ИБ обо всех случаях предоставления доступа третьим лицам к ресурсам ИС Учреждения.

11.5. Право удаленного доступа к ресурсам ИС Учреждения не предоставляется.

XII. Заключительные положения

12.1. В Положение могут быть внесены изменения и дополнения с целью приведения в соответствие определенных настоящим Положением защитных мер реальным условиям и текущим требованиям к защите информации и/или по результатам анализа инцидентов ИБ, актуальности, достаточности и эффективности используемых мер обеспечения ИБ, результатам проведения внутренних проверок ИБ и других контрольных мероприятий.

Приложение №1 к Положению об информационной безопасности

Реестр баз данных, подлежащих информационной защите:

1. 1С Бухгалтерия (компьютер инв. № 110104140434);
2. Крипто ПРО (компьютер инв. № 110104140434, компьютер инв. № 210104140001П);
3. База данных домена Microsoft (компьютер инв. № 110104140435);
4. Table Pro (компьютер инв. № 110104140433, компьютер инв. № 110134140122);
5. Перечень льготных профессий (компьютер инв. № 110104140432).