Рассмотрено на педагогическом совете
Протокол № 1
от 30.08.2019 г.

Утверждаю
Директор СОШ № 52
Н.Д. Джансариева

ПОЛОЖЕНИЕ
Об информационной безопасности учебно-воспитательного процесса

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с постановлением Правительства Кыргызской Республики № 295 от 17 июня 2019 года «О внесении изменений в некоторые решения Правительства Кыргызской Республики по вопросам повышения безопасности образовательной среды в общеобразовательных организациях», Типовым Положением «Об общеобразовательной организации», в соответствии с Концепцией создания информационной системы управления образованием в Кыргызской Республике .№ 1245/1 от 08.10.2015 г., Уставом школы.

1.2. В Положении определены требования к сотрудникам, ответственным за функционирование информационной системы персональных данных, степень их ответственности, структура системы и необходимый уровень защищенности.

1.3. Целью настоящего Положения является обеспечение безопасности объектов защиты школы от всех видов информационных угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных.

1.4. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

2. Цели и задачи информационной безопасности

2. 1. Основной целью организации системы информационной безопасности является осуществление мероприятий информационной безопасности, обеспечивающих защиту от несанкционированного доступа к информационным ресурсам школы.

2.2. Основными задачами обеспечения информационной безопасности являются:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализация права на доступ к информации;
- организация эксплуатации технических и программных средств защиты информации. Текущий контроль работы средств и систем защиты информации.
- организация и контроль резервного копирования информации.

3. Объект и структура действия Положения

3.1. Информационная система управления образованием (ИСУО) - комплекс, включающий вычислительное и коммуникационное оборудование, программное обеспечение, массивы данных, пользователей, процедуры, обеспечивающий сбор, обработку, хранение и распространение информации для удовлетворения

информационных потребностей руководителей системы образования, сотрудников системы образования и других заинтересованных лиц.

3.2. Информационная система управления образованием предназначена для сбора, хранения, распространения информации в системе образования, а также для автоматизации управленческой деятельности органов управления образованием всех уровней.

3.3. Основные функции и функциональные блоки ИСУО:

Система электронного документооборота и взаимодействия в системе образования Кыргызской Республики, должна обеспечить:

- регистрацию документа, позволяющую однозначно идентифицировать документ;
- хранение сведений о движении документа и возможность идентифицировать ответственного за исполнение документа или отдельной задачи данного документа в каждый момент времени жизни документа;
- хранение базы документной информации, позволяющей исключить возможность дублирования документов;
- хранение файлов документов;
- безопасность и защиту данных, а также систему разграничения прав доступа к документной информации и документам;
- эффективно организованную систему поиска документа;
- формирование системы отчетности по видам, атрибутам и статусам документов, позволяющей контролировать движение документов по процессам документооборота и принимать управленческие решения, основываясь на данных из отчетов;
- внутреннюю систему обмена электронными сообщениями между сотрудниками системы образования.

Система электронного документооборота ИСУО должна включать всех участников системы образования на всех уровнях.

4. Лица, ответственные за обеспечение информационной безопасности

4.1. Лица, ответственные за обеспечение информационной безопасности, в пределах своих функциональных обязанностей обеспечивают безопасность информации обрабатываемой, передаваемой и хранимой при помощи информационных средств в школе.

4.2. Лица, ответственные за информационную безопасность, выполняют следующие основные функции:

- разработка инструкций по информационной безопасности: инструкции по организации антивирусной защиты, инструкции по безопасной работе в Интернете.
- обучение работников-пользователей персональных компьютеров (далее по тексту - ПК) правилам безопасной обработки информации и правилам работы со средствами защиты информации.
- организация антивирусного контроля магнитных носителей информации и файлов электронной почты, поступающих в ОУ.
- текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации.
- контроль целостности эксплуатируемого на ПК программного обеспечения с целью выявления несанкционированных изменений в нём.
- контроль за санкционированным изменением программного обеспечения, заменой и ремонтом ПК.
- контроль пользования Интернетом.

5. Обязанности лиц, ответственных за обеспечение информационной безопасности школы

5.1. Обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах, возложенных на них обязанностей, выявлять нарушения и несанкционированные действия работников-пользователей ПК, а также принимать необходимые меры по устранению нарушений.
5.2. Проводить инструктаж работников-пользователей ПК по правилам работы с используемыми средствами и системами защиты информации.
5.3. Отслеживать работу антивирусных программ, проводить один раз в неделю полную проверку компьютеров на наличие вирусов.
5.4. Контролировать регулярное резервное копирование данных (не реже чем один раз в месяц) всеми пользователями ПК, иметь возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней.
5.5. Предотвращать несанкционированный доступ к информации и (или) передачи ее лицам, не имеющим права на доступ к информации.
5.6. Своевременно выявлять факты несанкционированного доступа к информации.
5.7. Предупреждать возможности неблагоприятных последствий нарушения порядка доступа к информации.
5.8. Не допускать воздействия на технические средства обработки информации, в результате которого нарушается их функционирование.
5.9. Постоянно контролировать обеспечение высокого уровня защищенности информации в школе.

6. Требования к сотрудникам по обеспечению защиты персональных данных

6.1. Все сотрудники школы, являющиеся пользователями ИСУО, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности персональных данных.
6.2. Сотрудники школы, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать несанкционированного доступа к ним, а также предупреждать возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.
6.3. Сотрудники школы должны следовать установленным процедурам поддержания режима безопасности персональных данных при выборе и использовании паролей (если не используются технические средства аутентификации).
6.4. Сотрудники школы должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности персональных данных и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.
6.5. Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.
6.6. Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами школы, третьим лицам.
6.7. При работе с персональными данными в ИСУО сотрудники ОУ обязаны обеспечить отсутствие возможности просмотра их третьими лицами с мониторов автоматизированных рабочих мест.

6.8. При завершении работы с информационной системой сотрудники обязаны защитить рабочее место или с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.
6.9. Сотрудники должны быть проинформированы об угрозах нарушения режима безопасности персональных данных и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили политику и процедуры безопасности персональных данных.
6.10. Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы с персональными данными, могущих повлечь за собой угрозы их безопасности, а также о выявленных ими событиях, затрагивающих безопасность персональных данных, руководству школы и лицу, отвечающему за немедленное реагирование на угрозы информационной безопасности.

7. Права ответственных лиц за обеспечение информационной безопасности

7.1. Требовать от работников-пользователей информационной системы безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению безопасности и защиты информации, содержащей сведения ограниченного распространения.
7.2. Готовить предложения по совершенствованию системы информационной безопасности школы.

8. Ответственность ответственных лиц за информационную безопасность

8.1. На лица, ответственные за информационную безопасность школы, возлагается персональная ответственность за качество проводимых ими работ по обеспечению информационной безопасности, защиты информации в соответствии с функциональными обязанностями, определёнными настоящим Положением.