УТВЕРЖДАЮ
Директор
Дж.Б.Саидинова

ПОЛОЖЕНИЕ
ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСТНОСТИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА АК-ТИЛЕКСКАЯ СОШ

1.Общие положения

1.1. Настоящее Положение разработано в соответствии с постановлением правительства КР от 17 июня 2019 года №295 «О внесении изменений в некоторые решения Правительства Кыргызской Республики по вопросам повышения безопасности образовательной среды в общеобразовательных организациях», согласно пункту 7, 14-2 Типового положения об общеобразовательной организации (в редакции постановлений Правительства КР от 2 октября 2013 года №544, 17 сентября 2014 года №535, 17 июня 2019 года №295), с Концепцией создания информационной системы управления образованием в Кыргызской республике от 8 октября 2015 года №1245/1.1.4.

1.2. Положение принимается решением педагогического совета образовательной организации, с учетом мнения профсоюзного комитета первичной профсоюзной образовательной организации, утверждается приказом директора. Изменения и дополнения в настоящее Положение вносятся решением педагогического совета ОО с учетом мнения профсоюзного комитета первичной профсоюзной организации.

1.3. В положении определены требования к персоналу информационной системы персональных данных, степень ответственности сотрудников, структура и необходимый уровень защищённости.

1.4. Целью настоящего Положения является обеспечение безопасности объектов защиты ОО от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных (УБПД).

1.5. 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.

1.6. Срок действия данного Положения не ограничен. Положение действует до принятия нового.

2.Область действия.

2.1. 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.

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

2.2. Создание ИСУО основывается на следующих принципах:

-однократный ввод и многократное использование первичной информации, в том числе для целей управления образования;
-использование структурного проектирования. ИСУО должна состоять из относительно самостоятельных функциональных подсистем;
-обеспечение совместимости информационных систем органов управления образования за счет использования единой системы классификации и кодировании;
-возможность интеграции систем образования между собой и с информационным ресурсами других ведомств в части совместного межведомственного использования персональных данных, статистических данных и электронного обмена документами;
-обеспечение системы информационной безопасности и защиты персональных данных в соответствии с требованиями законодательства КР;
-централизованное управления разработкой, внедрением и сопровождением ИСУО;
-создание подсистем ИСУО преимущественно в виде веб-приложений с доступом к работе через интернет;
-принятие решения о модернизации в разработке новых компонентов ИСУО с учетом максимально возможного сохранения существующих программно-технических средств;
-обеспечение расширяемости/масштабируемости ИСУО –возможности добавления новых функций или изменения некоторых уже имеющихся при неизменных остальных функциональных частях ИСУО;
-создание дружелюбного интерфейса пользователей ИСУО, не требующих специальной компьютерной подготовки пользователя;
-сопровождение функциональных возможностей ИСУО подробным справочным руководством;
-принцип непрерывного развития. ИСУО создается с учетом возможной необходимости внесения изменений в связи с постоянно изменяющимися условиями – изменениями в законодательстве, информационными технологиями и другими.

2.3. 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;
Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов;
(ИСПД) – информационная система, представляющая собой совокупность персональных данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств;
Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
Использование персональных данных – (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации;

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин; \

Персональные данные (ПД) – любая информация, относящаяся к определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отечество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с законами не распространяется требование соблюдения конфиденциальности;

Раскрытие персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неорганичного круга лиц, в т ом числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых, уничтожаются материальные носители персональных данных;

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации;

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации; целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения)

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы звукозаписи, звукоусиления, звуковоспроизведения переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации);

Программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах).

4. Цели и задачи информационной безопасности.

4.1. Цель: осуществление мероприятий информационной безопасности, обеспечивающих защиту от несанкционированного доступа к информационным ресурсам ОО.
4.2. 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.
-организация и контроль резервного копирования информация.

5.Ответственные лица за обеспечение информационной безопасности.

5.1. Ответственные лица за обеспечение информационной безопасности (далее по тексту – ответственные лица) в пределах своих функциональных обязанностей обеспечивают безопасность информации обрабатываемой, передаваемой и хранимой при помощи информационных средств в ОО.
5.2. Ответственные лица за информационную безопасность выполняют следующие основные функции:
-разработка инструкций по информационной безопасности: 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 ОО;
-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 нем;
-контроль за санкционированным изменением программного обеспечения, заменой и ремонтом ПК.
-контроль использования Интернетом.

6. Обязанности ответственных лиц за обеспечение информационной безопасности образовательной организации.

6.1. Обеспечивать функционирование и поддерживать работоспособность средств 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;
6.2. Совместно с программистами обслуживающих ОО (при наличии контракта, договора и т.д.), принимать меры по восстановлению работоспособности средств и систем защиты информации.
6.3. Проводить инструктаж работников-пользователей ПК по правилам работы с используемыми средствами и системами защиты информации;
6.4. Отслеживать работу антивирусных программ, проводить один раз в неделю полную проверку компьютеров на наличие вирусов;
6.5. предотвращать несанкционированный доступ к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
6.6. Своевременно выявлять факты несанкционированный доступа к информации.
6.7. Предупреждать возможности неблагоприятных последствий нарушения порядка доступа к информации;
6.8. Не допускать воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
6.9. Постоянно контролировать обеспечение высокого уровня защищенности информации в ОО.

7. Требования к сотрудникам по обеспечению защиты персональных данных.
7.1. Все сотрудники ОО, являющиеся пользователями ИСУО, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПД;
7.2. Сотрудников ОО, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать несанкционированного доступа (НСД) к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.
7.3. Сотрудники ОО должны следовать установленным процедурам поддержания режима безопасности ПД при выборе и использовании паролей (если не используются технические средства аутентификации).
7.4. Сотрудники ОО должны обеспечивать надлежащую защиту оборудованию, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПД и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.
7.5. Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.
7.6. Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами ОО, третьим лицам.
7.7. При работе с ПД в ИСУО сотрудники ОО обязаны обеспечить отсутствие возможности просмотра ПД третьими лицами с мониторов автоматизированном рабочем месте (АРМ).
7.8. При завершении работы с ИСПД сотрудники обязаны защитить АРМ или с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.
7.9. Сотрудники ОО должны быть проинформированы об угрозах нарушения режима безопасности ПД и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили политику и процедуры безопасности ПД.
7.10. Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПД, могущих повлечь за собой угрозы безопасности ПД, а также выявленных ими событиях, затрагивающих безопасность ПД, руководству ОУ и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПД.
8. Использование сети Интернет.
8.1. Использование сети Интернет в ОО осуществляется в целях образовательного процесса. В рамках развития личности, ее социализации и получения знаний в области компьютерной грамотности лицо может осуществлять доступ к ресурсам не образовательной направленности.
8.2. Использование сети Интернет в ОО подчинено следующим принципам:
-соответствия образовательным;
-способствования гармоничному формированию и развитию личности;
-уважения закона авторских и смежных прав, а также иных прав, а также иных прав, чести и достоинства других граждан и пользователей Интернета;
-приобретения новых навыков и знаний;
-расширения применяемого спектра учебных и наглядных пособий;
-социализации личности, введения в информационное общество.
8.3. Во время занятий контроль за использованием обучающимися сети Интернет в соответствии настоящим Правилами осуществлять учитель, ведущий занятие.
Учитель в процессе обучения:
-наблюдает за использованием компьютера и сети Интернет учащимися;

-запрещает дальнейшую работу учащегося в сети Интернет в случае нарушения учащимися настоящих правил и иных нормативных документов, регламентирующих использование сети интернет в образовательном учреждении;
-принимает предусмотренные настоящими правилами и иными нормативными документами меры для пересечения дальнейших попыток доступа к ресурсу/группе ресурсов, несовместимых с задачами образования;
-формирует у детей навыки самостоятельного и ответственного потребления информационной продукции;
-повышает уровень медиа грамотности детей;
-формирует у детей позитивную картину мира и адекватных базисных представлений об окружающем мире и человеке;
-приносит ценностное, моральное и нравственно-этическое и развитие детей;
-формирует информационную культуру, как фактора обеспечения информационной безопасности.

8.4. Сотрудники ОО вправе:

-размещать информацию в сети Интернет на Интернет-ресурсах ОО;
-иметь учетную запись электронной почты на Интернет-ресурсах ОО;
-включать родителей в совместную со ОО деятельность по обеспечению безопасности детей в Интернет пространстве.

8.5. Сотрудникам ОО запрещается размещать в сети Интернет и на образовательных ресурсах информацию:
-противоречащую требованиям законодательства КР и локальным нормативным актам ОО, не относящуюся к образовательному процессу и не связанную с деятельностью ОО;
-нарушающую нравственные и этические нормы, требования профессиональной этики.

8.6. Обучающиеся ОО вправе:
- использовать ресурсы, размещенные в сети Интернет, в том числе Интернет-ресурсы ОО, в порядке и на условиях, которые предусмотрены настоящим Положением.
-размещать информацию и сведения на Интернет-ресурсах ОО.
-получать правовые знания в области информатизации в ОО.
-владеть знаниями о защите компьютера от вредоносных программ, о нелегальном, пиратском контенте и об опасности его скачивания.

9. Обучающемся запрещается:
9.1. Находиться на ресурсах, содержание и тематика которых недопустима для несовершеннолетних и/или нарушает законодательство КР, а именно:
-побуждающая обучающихся к совершению действия. Представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью;
-способная вызвать у обучающихся желание употребить наркотические средства, психотропные и одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию;
-обосновывающая или оправдывающая допустимость насилия и жестокости, либо побуждающая осуществлять насильственные действия по отношению к людям или животным;
-отрицающая семейные ценности;
-оправдывающая противоправное поведение;
-осуществлять любые сделки через интернет;
-загружать файлы на компьютер ОО без разрешения ответственного лица;
-распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы;
-посещение сайтов, пропагандирующих экстремизм и формы поведения, отклоняющиеся от общепринятых норм.

9.2. Пользователи сети Интернет в ОО должны учитывать, что технические средства и программное обеспечение не могут обеспечить полную фильтрацию ресурсов сети Интернет вследствие частого обновления ресурсов. В связи с этим существует опасность обнаружения обучающимися ресурсов, содержание которых противоречит законодательству КР и не совместимо с целями и задачами образовательного процесса не на Интернет – ресурсах ОО. Участникам использования сети Интернет следует осознавать, что школа не несет ответственности за случайный доступ к подобной информации, размещенной на других Интернет-ресурсах.

9.3. Если в процессе работы пользователем будет обнаружен ресурс, содержимое которого не совместимо с целями образовательного процесса, он обязан незамедлительного сообщить об этом ответственному лицу с указанием интернет-адреса (URL) и покинуть данный ресурс.

10.Права ответственных лиц за обеспечение информационной безопасности.

10.1. Требовать от работников – пользователей ПК безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению безопасности и защиты информации, содержащей сведения ограниченного распространения;

10.2. Готовить предложения по совершенствованию системы информационной безопасности ОО.

1.1.Ответственность ответственных лиц за информационную безопасность.

11.1. На ответственных лиц за информационную безопасность ОО возлагается персональная ответственность за качество проводимых ими работ по обеспечению информационной безопасности ОО, защиты информации в соответствии с функциональными обязанностями, определенными настоящим Положением.