КГУ «Рудненская специальная школа для детей с особыми образовательными потребностями» Управления образования акимата Костанайской области

РАССМОТРЕНО
на заседании педагогического Совета
от 27.02.2023г.
протокол №8

УТВЕРЖДАЮ
Директор школы
Дайкер А.А.
27.02.2023г.

ПОЛИТИКА ИНФОМАЦИОННОЙ БЕЗОПАСНОСТИ

КГУ «Рудненская специальная школа для детей с особыми образовательными потребностями» Управления образования акимата Костанайской области

2023 г.

1. Общие положения

1.1. Политика информационной безопасности КГУ «Рудненская специальная школа для детей с особыми образовательными потребностями» Управления образования акимата Костанайской области (далее-школа) определяет цели и задачи системы обеспечения единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности (далее – ЕТ) и устанавливает совокупность правил, процедур, практических приёмов, требований и руководящих принципов, которыми руководствуются работники и обучающиеся школы при осуществлении своей деятельности с использованием технических и программных сред школы.

1.2. Основной целью Политики информационной безопасности школы является установление обязательных для исполнения требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности школы, при осуществлении уставной деятельности, которая предусматривает принятие необходимых мер в целях защиты информации от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в управлении и соответствия её требованиям и нормам, определённых государственными стандартами

1.3. Политика **информационной безопасности** разработана в соответствии с:

Дата и номер	Содержание
Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832	«Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»
Постановление Правительства Республики Казахстан от 18 июня 2018 года № 355	«О внесении дополнений и изменений в постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»
Закона Республики Казахстан от 24 ноября 2015 года №418-V	"Об информатизации"
Закон Республики Казахстан от 21 мая 2013 года N 94-V.	«О персональных данных и их защите»
Закон Республики Казахстан от 7 января 2003 года № 370-II	Об электронном документе и электронной цифровой подписи

Закон Республики Казахстан от 18 февраля 2005 года № 31-III	«О противодействии экстремизму»
Закон Республики Казахстан от 21 мая 2013 года № 95-V	«О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам персональных данных и их защиты»
Приказ МП Республики Казахстан от 26 января 2023 года №20	«О внесении изменений в приказ Министра просвещения Республики Казахстан от 14 ноября 2022 года №456 «Об утверждении минимальных требований к объектам информатизации в области образования»

а также рядом иных сопутствующих нормативных правовых актов в сфере защиты информации.

1.4. Выполнение требований Политики ИБ является обязательным для всех структурных подразделений школы.

1.5. Ответственность за соблюдение информационной безопасности несет каждый сотрудник и обучающийся школы.

2. Цель и задачи политики информационной безопасности

2.1. Основными **целями** политики ИБ являются:

- сохранение конфиденциальности критичных информационных ресурсов;
- обеспечение непрерывности доступа к информационным ресурсам школы;
- защита целостности информации с целью поддержания возможности школы по оказанию услуг высокого качества и принятию эффективных управленческих решений; - повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами школы;
- определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в управлении.
- повышение уровня эффективности, непрерывности, контролируемости мер по защите от реальных угроз ИБ;
- защита пользователей от вредоносного несанкционированного воздействия со стороны;
- выполнение норм и требований законодательных и подзаконных актов в области информатизации.
- предотвращение и/или снижение ущерба от инцидентов ИБ.

2.2. Основными **задачами** политики ИБ являются:

- разработка требований по обеспечению ИБ;
- контроль выполнения установленных требований по обеспечению ИБ;
-повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию ИБ;
- разработка нормативных документов для обеспечения ИБ школы;
-выявление, оценка, прогнозирование и предотвращение реализации угроз ИБ школы;
- организация антивирусной и межсетевой защиты информационных ресурсов школы;
- защита информации школы от несанкционированного доступа (далее - НСД) и утечки по техническим каналам связи;
- организация периодической проверки соблюдения информационной безопасности с последующим представлением отчёта по результатам указанной проверки директору школы.
- ограничение доступа к нежелательной и вредоносной информации.
- периодическое информирование сотрудников и обучающихся школы о существующих угрозах информационного характера.

3. Концептуальная схема обеспечения информационной безопасности

3.1. Политика ИБ школы направлена на защиту информационных ресурсов (активов) от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий сотрудников и обучающихся школы-интернат, технических сбоев автоматизированных систем, неправильных технологических и организационных решений в процессах поиска, сбора хранения, обработки, предоставления и распространения информации и обеспечение эффективного и бесперебойного процесса деятельности.

3.2. Наибольшими возможностями для нанесения ущерба обладают сами пользователи информационной системы школы. Риск аварий, программных и технических сбоев в автоматизированных системах определяется состоянием аппаратного и программного обеспечения, надёжностью систем энергосбережения, квалификацией сотрудников, степенью защищенности программно-аппаратных комплексов от вредоносного воздействия программным обеспечением и способностью к правильным действиям в критичных ситуациях.

3.3. Стратегия обеспечения ИБ школы заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно - технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий сотрудников школы, а также информационному воздействию на пользователей ИС.

3.4. Максимально оградить работников и обучающихся от воздействия нежелательного и запрещённого информационного потока, применяя различные программно-электронный технические решения.

4. Основные принципы обеспечения информационной безопасности.

Основными принципами обеспечения ИБ:

4.1. разработка системы информационной безопасности в соответствии с существующими законодательными требованиями и нормативными актами в области информационной безопасности;

4.2. постоянный и всесторонний анализ автоматизированных систем, трудового и учебного процесса с целью выявления уязвимостей в работе информационной системы школы;

4.3. своевременное обнаружение проблем, потенциально способных повлиять на ИБ школы-интернат, корректировка моделей угроз и нарушителя;

4.4. разработка и внедрение защитных мер;

4.5. контроль эффективности принимаемых защитных мер;

4.6. персонификация и разделение ролей и ответственности между сотрудниками и обучающимися школы за обеспечение ИБ школы исходит из принципа персональной и единоличной ответственности за совершаемые действий, в соответствии с требованиями данной концепции.

5. Объекты защиты

5.1. Объектами защиты с точки зрения ИБ в управлении являются:

- информационный процесс профессиональной деятельности;
- информационные активы школы;
- информационный учебный процесс.

5.2. Защищаемая информация делится на следующие виды:

- информация по финансово-экономической деятельности школы;
- персональные данные – любая информация, относящаяся к определённому или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
- другая информация, не относящаяся ни к одному из указанных выше видов, которая отмечена грифом «Для служебного пользования» или «Конфиденциально».

6. Требования по информационной безопасности.

Для комплексной и эффективной реализации описанных целей и задач, информационную среду школы целесообразно рассматривать как набор отдельных взаимосвязанных областей, каждая из которых имеет свои требования в части обеспечения информационной безопасности.

В соответствии с данным подходом информационная среда школы разделена на следующие области:

6.1. Политика локальной вычислительной сети. Политика сетевого администрирования.

В настоящем разделе применены термины и использованы ссылки на следующие стандарты Республики Казахстан СТ РК 2190-2012:
"Информационные технологии. Интернет-ресурсы государственных органов и организаций. Требования", СТ РК 2191-2012
"Информационные технологии. Доступность Интернет-ресурса для людей с ограниченными возможностями", СТ РК 2192-2012
"Информационные технологии. Интернет-ресурс, интернет-портал, интранет-портал. Общие описания", СТ РК 2193-2012
"Информационные технологии. Рекомендуемая практика разработки мобильных веб-приложений", СТ РК 2199-2012
"Информационные технологии. Требования к безопасности веб-приложений в государственных органах".

Общие понятия

1. Локальная вычислительная сеть образовательного учреждения (далее ЛВС) представляет собой организационно-технологический комплекс, созданный для реализации взаимодействия вычислительных и информационных ресурсов ОУ с глобальными сетями телекоммуникаций.
2. Локальная вычислительная сеть образовательного учреждения обеспечивает возможность выхода пользователей во внешние сети и удаленный доступ для пользователей к общим информационным и вычислительным ресурсам учреждения и других образовательных учреждений.
3. Локальная вычислительная сеть образовательного учреждения является технической и технологической основой эффективного функционирования информационных узлов (серверов) ОУ, обеспечивающих информационную поддержку научной, методической и преподавательской деятельности сотрудников системы образования, включая систему документооборота, а также сферу административного управления.

Основные задачи функционирования ЛВС школы и распределение обязанностей

- создание, развитие и обеспечение функционирования организационной, технической, программно-методической и технологической информационной инфраструктуры в целях использования глобальных телекоммуникационных сетей для информационного обеспечения научной, методической, преподавательской деятельности, а также административного управления;
- обеспечение информационного межсетевого взаимодействия в рамках выполняемых проектов.

Понятие ЛВС:

Локальная сеть (ЛВС) – организационно-технологический комплекс, состоящий из следующих функциональных частей:

1) средства доступа к глобальным сетям и передачи информации;
2) средства защиты информации (межсетевые экраны как аппаратные, так и программные);
3) средства коммутации (коммутаторы, хабы);
4) серверное оборудование;
5) рабочие места на базе персональных компьютеров.

Управление работой сети включает в себя:

1) обеспечение информационной безопасности;
2) управление информационным обменом локальной сети с внешними сетями телекоммуникаций;
3) управление информационными потоками внутри локальной сети;
4) регистрацию информационных ресурсов и их разработчиков;
5) управление доступом к информационным ресурсам;
6) управление процессами размещения и модификации информационных ресурсов;
7) регистрацию (подключение и отключение) рабочих мест;
8) регистрацию Пользователей сети и Администраторов, определение их полномочий и прав по доступу к сетевым, информационным и вычислительным ресурсам данной сети;
9) выбор используемых в локальной сети программных инструментальных средств;
10) разрешение конфликтных ситуаций «Пользователь – сеть».

Информационная безопасность ЛВС ОУ обеспечивается путём:

1) использования технических, технологических, программных и организационных средств защиты вычислительных программных и информационных ресурсов сети от попыток причинения вреда, ущерба или несанкционированного доступа;

2) использования обязательной регистрации и документирования информационных ресурсов сети; допускается разграничение прав доступов на основании сетевых и локальных списков учётных записей;
3) осуществления Системными администраторами мер по разграничению доступа к информационным ресурсам Корпоративной сети, путём определения конфигураций и настроек программного, технического и сетевого обеспечения.
4) Предоставление доступа к ресурсам сети ИНТЕРНЕТ для работников и обучающихся школы возможно производить либо на основании фиксированных адресов закреплённых рабочих станций, либо путём проведения авторизации при прохождении авторизации. Доступ к ресурсам сети ИНТЕРНЕТ для обучающихся производится исключительно на основании результатов авторизации;
5) использования резервного копирования информационных ресурсов сети в целях обеспечения их сохранности.

В целях обеспечения информационной безопасности Системный администратор сети обязан контролировать трафик, адресацию и источники сообщений, приходящих в сеть и исходящих из нее, выявлять и идентифицировать попытки несанкционированного доступа к ресурсам сети.

Функции Системного администратора локальных сетей:

1. Администратор локальной сети принимает меры к обеспечению работоспособности и информационной безопасности локальной сети. Администратор локальной сети обязан поддерживать заданные настройки программного обеспечения и технического оборудования, выполнять рекомендации по установке программного обеспечения на серверах и компьютерах локальной сети.

2. Системные администраторы локальных сетей ОУ обеспечивают:

- работоспособность технических, сетевых ресурсов и информационную безопасность сети;
-выполняет регистрацию Пользователей сети; фиксирует полномочия и права доступа к сетевым, информационным ресурсам сети.
-создание и поддержку единой технической, программно-методической и технологической инфраструктуры локальных сетей;
-документирование и регистрацию информационных ресурсов сети и разработчиков информационных ресурсов, размещение информационных ресурсов и прекращение доступа к ним;
-организационное и технологическое обеспечение выхода пользователей во внешние сети и доступа извне к информационным и вычислительным ресурсам локальных сетей через информационные узлы;
-создание и модификацию баз информационных ресурсов;

- создание учетных записей пользователей; отключение и регистрацию рабочих мест пользователей; подключение, отключение и тестирование правильности настроек серверов и маршрутизаторов локальных сетей, входящих в состав сети;
- предотвращение несанкционированного доступа извне к ресурсам сети; проведение учебной и консультативной работы с пользователями локальных сетей.

Эксплуатация программного обеспечения для регистрации, анализа, обработки и учета данных о пользователях.

Пользователи ЛВС школы, их права и обязанности

Пользователями сети являются сотрудники либо обучающимися образовательного учреждения, прошедшие установленную процедуру регистрации в качестве Пользователей.

В ходе регистрации за каждым Пользователем закрепляется имя, пароль и одно или несколько определенных рабочих мест, в зависимости от необходимых требований.

Пользователь сети обязан:

- использовать доступ к локальным и глобальным сетям только в профессиональных и служебных целях;
- не использовать информационные и технические ресурсы сети в коммерческих целях и для явной или скрытой рекламы услуг, продукции и товаров любых организаций и физических лиц, за исключением образовательных услуг, а также продукции и товаров, предназначенных для обеспечения образовательного процесса;
- исключить возможность неосторожного причинения вреда (действием или бездействием) техническим и информационным ресурсам сети;
- не предпринимать попыток несанкционированного доступа к информационным и вычислительным ресурсам локальных и глобальных сетей, доступ к которым осуществляется через сеть (в том числе, не пытаться бесплатно или за чужой счет получить платную информацию);
- перед использованием или открытием файлов, полученных из других источников, проверять файлы на наличие вирусов;
- не использовать доступ к Корпоративной сети для распространения и тиражирования информации, распространение которой преследуется по закону, заведомо ложной информации и информации, порочащей организации и физические лица, а также служебной информации.
- не распространять ни в какой форме (в том числе, в электронном или печатном виде) информацию, приравненную к служебной информации, полученную из информационных ресурсов сети.

Пользователи имеют право на:

- размещение своего почтового ящика на одном из почтовых серверов Корпоративной сети в установленном порядке, при наличии такового;

• получению доступа к личному или общему хранилищу данных в ЛВС;

• обращение к платной информации имеющейся в глобальной сети с разрешения руководителя Образовательного учреждения. В этом случае пользователи оплачивают получаемые ими услуги самостоятельно и предоставляют документы, подтверждающие оплату.

Пользователям сети запрещено:

• использование программ, осуществляющих сканирование сети (различные снифферы, сканеры портов и тому подобные действия, без письменного предупреждения системного администратора с объяснением служебной необходимости подобных действий);
• установка дополнительных сетевых протоколов, изменение конфигурации настроек сетевых протоколов без ведома системного администратора;
• за исключением случаев, связанных со служебной необходимостью, просматривать видео через сеть;
• за исключением случаев, связанных со служебной необходимостью, отправлять по электронной почте большие файлы (особенно музыку и видео);
• открывать файлы и запускать программы на локальном компьютере из непроверенных источников или принесённых с собой на переносных носителях без предварительного сохранения на локальном жестком диске и последующей проверкой антивирусной программой;
• хранение на публичных сетевых дисках файлов, не относящихся к выполнению служебных обязанностей сотрудника (игрушки, видео, виртуальные CD и т.п.);
• просматривать сайты порнографической, развлекательной направленности, и сайты содержание которых не относится впрямую к служебным обязанностям работника;
• использование программ для зарабатывания денег в сети Интернет;

• скачивание музыкальных и видео файлов, а так же файлов, не имеющих отношения к текущим служебным обязанностям работника;
• открывать на локальном компьютере приложения к почте из непроверенных источников без предварительного сохранения на локальном жестком диске и последующей проверкой антивирусной программой.

Пользователь сети может получать доступ к ресурсам локальной и глобальной сети только под своими именем и паролем, полученными в ходе регистрации Пользователя сети. Передача Пользователем имени и пароля другому лицу запрещена.

Порядок регистрации и перерегистрации пользователей ЛВС школы

1. Регистрация Пользователя Корпоративной сети производится бессрочно либо сроком на один учебный год.
2. В ходе регистрации определяются сетевое имя Пользователя и его пароль.

3. Регистрация Пользователя сети аннулируется:

• по представлению руководителя образовательного учреждения, в котором работает Пользователь;

• по представлению Системного администратора сети в случае нарушения Пользователем требований настоящей политики и одноимённого положения;

• в связи с прекращением трудовых отношений.

4. В случае прекращения регистрации Пользователя в связи с прекращением трудовых отношений, руководитель образовательного учреждения, в котором работает Пользователь извещает об этом системного администратора не менее, чем за неделю до даты увольнения.

Ответственность,возникающая в связи с функционированием ЛВС школы

1. Пользователь сети, за которым закреплено определенное рабочее место, несет ответственность за соблюдение установленных настоящим Положением требований. Пользователь сети обязан при невозможности обеспечить выполнение требований данногоПоложения немедленное информирование об этом Системного администратора сети (по электронной почте, письменно, по телефону или лично).

2. Администратор сети обо всех случаях нарушения настоящего Положения обязан в письменном виде информировать руководителя школы, в котором работает пользователь-нарушитель.

3. При систематическом нарушении требований настоящего Положения Пользователями конкретного подразделения производится отключение зарегистрированного рабочего места (локальной сети) соответствующего подразделения (пользователя) от Корпоративной сети.

4. В случае возникновения ущерба или причинения вреда имуществу, правам, репутации в результате деятельности Пользователя(ей) сети, возмещение ущерба является обязанностью пользователя(ей), чьи действия послужили причиной возникновения конкретного ущерба или вреда. Такое возмещение производится добровольно или по решению суда в соответствии с действующим законодательством РК.

Действие настоящего раздела Положения распространяется на лиц, работающих или обучающихся в образовательном учреждении, зарегистрированных в качестве Пользователей сети. Процедуры управления корпоративной сетью определяются на основании положения об использовании корпоративной сети, дополнений к положению об использовании корпоративной сети и приказов.

6.2. Управление пользователями. Работа пользователей.

Основные требования заключается:

- В определении основных правил работы пользователей с компьютерной техникой и корпоративной информационной системой для поддержания необходимого уровня информационной безопасности в школе.
- В информировании пользователя о том, что любые его действия в корпоративной информационной системе или работа на любом компьютере, входящем в его в ее состав, могут быть и будут запротоколированы и использованы в дальнейшем для проведения расследования причин компрометации системы.

Основные положения раздела:

1. Пользователю разрешается выполнять только те действия в корпоративной информационной системе, которые явно разрешены соответствующими политиками информационной безопасности.
2. Основные требования к управлению программным обеспечением определяются политикой безопасности «Управление программным обеспечением»
3. Всем сотрудникам и обучающимся запрещается создавать или использовать программное обеспечение, модули для программного обеспечения, включенного в перечень разрешенного ПО, в том числе составные части операционных систем, реализующие следующие функции:
   3.1. Нарушение работы серверов или рабочих станций, активного оборудования или отдельных элементов информационных систем;
   3.2. Перехватывание/подмена сетевого трафика;
   3.3. Получение несанкционированного доступа к серверам, рабочим станциям информационных систем, используя уязвимости или недокументированные функции;
   3.4. Запрещается преодолевать любые системы защиты, направленные на разграничение прав доступа, защиты информации составляющей коммерческую тайну, содержащей персональные данные и т.д.;
   3.5. Пользователь должен блокировать компьютер, в случае необходимости оставить без присмотра свое рабочее место, если компьютер не блокируется автоматически;
   3.6. Компьютер автоматически блокируется при простое более 10-15 минут.

Требования к аппаратному обеспечению:

1. Изменение конфигурации аппаратного обеспечения рабочих станций производится по заявке пользователя, согласованной с ответственным за информационную безопасность ИС и системным инженером.

2. Внесение изменений в конфигурацию рабочих станций школы осуществляет ответственный специалисты, осуществляющие поддержку ИТ инфраструктуры школы;
3. Несанкционированное изменение аппаратной конфигурации рабочих станций запрещено и виновное в нарушении лицо может быть привлечено к дисциплинарной ответственности.
4. Доступ к внутренним и внешним сервисам для сотрудников и обучающихся школы осуществляется ранее определённых разрешений доступов.

Пересечение с иными структурными частями ИБ:

1. Требования по использованию электронной почты определены в положении «Об использовании электронной почты в школе»;
2. Требования по использованию сети Интернет определены в положении «Об использовании сети ИНТЕРНЕТ в школе»
3. Требования по использованию антивирусной защиты определены в положении «Об антивирусной защите в школе»
4. Требования по обработке персональных данных определены в положении «Об использовании персональных данных»
5. Требованияпри работе с системой ЭЦП определеныв соответствии с рекомендациями удостоверяющих центров.

Права и обязанности пользователей ИС школы:

1. Требовать постоянной работоспособности рабочей станции;
2. Требовать изменения конфигурации рабочей станции в установленном порядке;
3. Требовать предоставления ИТ сервиса для выполнения своих должностных и учебных обязанностей в установленном порядке.
4. В случае конфликтных ситуаций обращаться к руководству администраторов всех уровней, а также непосредственно к лицу ответственному за информационную безопасность.
5. Пользователь обязан выполнять все требования данного пункта политики безопасности школы, имеющие отношение к их служебной и учебной деятельности.

6.3. Управление электронной почтой

Общие положения заключаются в :

1. определении ответственности пользователей за неправильное использование корпоративной системы электронной почты, а также потенциальные последствия

нарушения данных требований;

2. информировании пользователей о том, что, используя корпоративную электронную почту, они соглашаются выполнять требования данного раздела политики информационной безопасности и отказываются от любых прав на конфиденциальность сообщений созданных, посланных или полученных с использованием корпоративной системы электронной почты.

3. устанавливаются следующие требования к электронному почтовому обороту школы:

-Электронная почта – используется только для выполнения работником его служебных обязанностей;

-Сервисы электронной почты должны удовлетворять требованиям о географическом расположении и хранении персональных данных;

-Единственно возможный способ работы с электронной почтой в школе:

- использование корпоративной электронной почты. Работа с другими сервисами электронной почты, включая, но не ограничиваясь, бесплатными почтовыми серверами, только при согласовании с системным администратором школы-интернат;

- Запрещается рассылка цепных сообщений, спама, исполняемых файлов, файлов развлекательного характера;

-Запрещается использовать корпоративную электронную почту для любой деятельности с целью получения личной материальной выгоды.

-Запрещается пересылка и получение электронной почты, содержащей лицензионное программное обеспечение и другие действия, позволяющие обойти лицензионные соглашения или нарушить авторские права

-Запрещается посылать письма, содержащие информацию, составляющие коммерческую тайну школы. Исключения составляют пользователи, имеющие на это право в соответствии с положением «О коммерческой тайне»

-Запрещается создание и пересылка зашифрованных писем или писем, содержащих шифрованные участки, вложения, а также предпринимать любые другие действия затрудняющие анализ тела письма и его вложений. Исключение составляют пользователи, имеющие на это право в соответствии с положением «О коммерческой тайне».

-Запрещается создавать, отсылать письма дискредитирующей кого-либо информации, непристойного или вызывающего содержания, которая может быть воспринята, как преследование или умаление над расой, цветом кожи, национальностью, полом, сексуальной ориентацией, возрастом, религиозными или политическими предпочтениями. В случае получения такого письма пользователем,

оно должно быть немедленно удалено.

-При работе с электронной почтой на компьютере обязательно должно быть установлено корпоративное антивирусное программное обеспечение.

-При получении письма с вложением, каждый пользователь должен следовать процедуре, описанной в "Положении о работе с электронной почтой школы".

-Запрещается использование чужих адресов электронной почты, а также разрешать использование своего адреса кому-либо еще.

-Запрещается вести служебнуюпереписку,используюне официальную электронную почту.

Детальная процедура назначения ответственных, правила обработки писем при получении описана в положении "Об использовании электронной почты в школе" и приказах школы.

6.4. Управление программным обеспечением. Ответственность за использование вычислительной техники.

Основные положения раздела:

6.1. ПО (программное обеспечение) обеспечивает выполнение для КГУ «Рудненская специальная школа для детей с особыми образовательными потребностями» Управления образования акимата Костанайской области (далее школа) информационных функций, ради которых оно было приобретено.

6.2. Цель данного раздела политики информационной безопасности – формирование требований соблюдения лицензионных соглашений и запрещение на использование программного обеспечения с нарушением лицензионного законодательства (контрафактного) при использовании программного обеспечения. Определение требований контроля над использованием ПО со свободной лицензией.

6.3. Область действия данного раздела политики распространяется на всех пользователей школы, сотрудников, учителей, администрацию, иной персонал и обучающихся.

6.4. Набор и конфигурация программного обеспечения рабочих станций и серверов, установка программного обеспечения осуществляется только ответственными сотрудниками за сопровождение программного обеспечения, и определяется в соответствии с действующими положениями информационной безопасности, а также ролями и полномочиями пользователей.

6.5. Изменение лицензионного набора программного обеспечения, соответствующего роли пользователя, осуществляется администраторами по заявке

пользователя, согласованной с начальником подразделения пользователя или ответственным за развитие ИТ инфраструктуры.

6.6. Все программное обеспечение идентифицируется в реестре разрешенного программного обеспечения (регламентируется положением об использовании ПО).

6.7. К использованию в информационной системе школы допускается только программное обеспечение, внесенное в реестр разрешенного программного обеспечения.

6.8. Реестр программного обеспечения содержит лицензионное программное обеспечение и свободно распространяемое ПО, прошедшее проверку на отсутствие вредоносного кода, ответственным за информационную безопасность. Требований на формат данных реестра не накладывается.

6.9. Реестр программного обеспечения может быть изменен по решению ответственного за развитие ИТ инфраструктуры о приобретении и использовании нового программного обеспечения и после проверки на отсутствие вредоносного кода для бесплатного ПО.

6.10.Заявка на изменение реестра разрешенного ПО со свободно распространяемой лицензией оформляется на ответственного за ИТ инфраструктуру. Ограничений на использование бесплатного ПО не существует. Заявка на изменение разрешенного программного обеспечения содержит: полное наименование программного обеспечения и его производителя, описание функциональной направленности программного обеспечения, обоснование для использования программного обеспечения, ссылку на ресурс Интернет, где размещено программное обеспечение и подробная информация о нем.

6.11. Заявка на изменение реестра разрешенного лицензионного ПО оформляется на ответственного за ИТ инфраструктуру, в лице заместителя директора по ИКТ. Заявка на изменение разрешенного программного обеспечения содержит: полное наименование программного обеспечения и его производителя, описание функциональной направленности программного обеспечения, обоснование использования программного обеспечения. Служба, ответственная за поддержку ИТ инфраструктуры (отдел ИТ), при возможности приобретения, приобретает ПО, устанавливает ПО и осуществляет контроль за использованием лицензий.

6.12. Несанкционированное изменение конфигурации лицензионного программного обеспечения пользователями запрещено.

6.13. Ограничений на использование бесплатного ПО не накладывается. Ответственность за установку бесплатного ПО несет ответственный за сопровождение ПО, ответственность за работу данного типа ПО несут сами пользователи.

6.14. Периодически, но не реже одного раза в год, ответственный за ведение реестра разрешенного ПО, выполняет проверку на соответствие установленного ПО на компьютерах школы, внесенного в реестр.

6.15. Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары, коммуникационное оборудование, для целей настоящей политики вместе именуются "компьютерное оборудование". Компьютерное оборудование, предоставленное управлением, является ее собственностью и предназначено для использования исключительно в производственных целях.
6.16. Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности. Запрещается самостоятельно вносить какие-либо корректировки в аппаратную и программную составляющую используемого школьного оборудование. Любые изменения конфигурации оборудования проводятся исключительно ответственным работником школы-интерната.
6.17. Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавиши и после выхода из режима "Экранной заставки". Для установки режимов защиты пользователь должен обратиться к администратору ЛВС. Данные не должны быть скомпрометированы в случае халатности или небрежности приведшей к потере оборудования. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

Подробное определение норм и требований, а также законодательных актов, относительно использования того или иного программного обеспечения в школе, определены в политике школы об использовании ПО в школе.

6.5. Антивирусная защита

Общее понятие:

1. Антивирусное ПО – программное обеспечение, предназначенное для защиты от вредоносных программ посредством обнаружения зараженных программных модулей и системных областей, распознания и блокировки вирусных сигнатур, а также для восстановления исходного состояния зараженных объектов.

2. Вирус (компьютерный) – вредоносная программа, способная создавать свои копии или другие вредоносные программы и внедрять их в файлы, системные области компьютера, распространяться через компьютерные сети, а также осуществлять другие деструктивные действия.

3. Ответственными за ИТ инфраструктуру школы в области информационных технологий (системный администратор) определяется стандартный состав корпоративного антивирусного программного обеспечения. Установка иного антивирусного программного обеспечения не допускается.
4. Антивирусное программное обеспечение должно быть установлено, настроено и активировано на всех программно-технических средствах, имеющих доступ к информационным активам школы до начала их использования или подключения к информационным ресурсам.
5. Все возможные каналы поступления вредоносного программного обеспечения в информационно-технологическую инфраструктуру школы должны быть определены, проанализированы и защищены средствами антивирусной защиты.
6. Контролю на предмет обнаружения вредоносных программ должна подвергаться вся информация, создаваема и обрабатываемая программно-техническими средствами школы, а также принимаемая (передаваемая) посредством сменных носителей информации и средствами телекоммуникаций.
7. С целью эффективной борьбы с новыми видами зловредного программного обеспечения и уменьшения накладных расходов на администрирование должно выполняться централизованное, регулярное обновление всех средств антивирусной защиты, используемых для защиты информационных систем школы.

8. Для эффективной реализации АВЗ школы, необходимо:
   - унифицировать антивирусное программное обеспечение с возможностью централизованного управления.
   - постоянное, своевременное обновление антивирусных баз и программных компонентов.

   Реализацию данного пункта политики безопасности осуществляет системный администратор, контроль за исполнением обеспечивает ответственный за информационную безопасность.
9. Любые информационные системы, используемые в ЛВС школы или подключаемые к ней как локально, так и удаленно, в ходе эксплуатации должны подвергаться непрерывному антивирусному мониторингу и сканированию. К таковым системам относятся сервера и рабочие станции ЛВС школы, а также мобильные и отдельные автономные автоматизированные рабочие места руководства, сотрудников института и врачей-курсантов, имеющие доступ к информационным активам школы.

Порядок установки, настройки и проведения периодической проверки информационной системы антивирусным программным обеспечением определяется в положении «Об использовании антивирусного программного обеспечения». Какие-либо дополнения производятся исключительно ответственным за информационную безопасность школы.

6.6. Порядок обработки ПДн

Основные понятия:

Персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Информация — сведения (сообщения, данные) независимо от формы их представления.

Оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемые с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники.

Предоставление персональных данных — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Распространение персональных данных — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, когда обработка необходима для уточнения персональных данных).

Уничтожение персональных данных — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Персональные данные обрабатываются в школе в целях:

- обеспечения соблюдения Конституции Республики Казахстан, законодательных и иных нормативных правовых актов Республики Казахстан, локальных нормативных актов школы;
- осуществления функций, полномочий и обязанностей, возложенных законодательством Республики Казахстан на школу, в том числе по предоставлению персональных данных в органы государственной власти, в Пенсионный фонд Республики Казахстан, в Фонд социального страхования, а также в иные государственные органы;
- регулирования трудовых отношений с работниками школе (содействие в трудоустройстве, обучение и продвижение по службе, обеспечение личной безопасности, контроль количества и качества выполняемой работы, обеспечение сохранности имущества);
- предоставления работникам школы и членам их семей дополнительных гарантий и компенсаций, в том числе государственного пенсионного

обеспечения, добровольного медицинского страхования, медицинского обслуживания и других видов социального обеспечения;
- обеспечения проведения учебного процесса.

Меры, принимаемые в школе для обеспечения выполнения обязанностей оператора при обработке персональных данных:
- хранение электронных копий носителей персональных данных с соблюдением условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним;
- осуществление внутреннего контроля соответствия обработки персональных данных на основании Закона Республики Казахстан от 21 мая 2013 года N 94-V, и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным нормативным актам школы;
- иные меры, предусмотренные законодательством Республики Казахстан в области персональных данных.

Меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются в соответствии с локальными нормативными актами школы, регламентирующими вопросы обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных в школе.

6.7. Использование Электронной цифровой подписи

Основные понятия:
- **Носитель ключевой информации** – носитель информации (дискета, флэш-память, и прочие носители) на которых храниться электронный ключ, предназначенный для защиты электронных взаимодействий.
- **ЦУКС** - центр управления ключевыми системами место изготовления носителя ключевой информации НКИ.
- **Секретный (закрытый) ключ подписи** - ключ предназначенный для формирования им электронной цифровой подписи электронных документов.
- **Открытый (публичный) ключ подписи** - ключ, автоматически формируется при изготовлении секретного ключа подписи и однозначно зависящий от него.

Открытый ключ предназначен для проверки корректности электронной цифровой подписи электронного документа. Открытый ключ считается принадлежащим участнику электронных взаимодействий, если он был сертифицирован (зарегистрирован) установленным порядком.

- **Ключ шифрования** - ключ предназначенный для закрытия электронного документа при электронных взаимодействиях.
- **Шифрование** - специализированный метод защиты информации от ознакомления с ней третьих лиц, основанный на кодировании информации с использованием соответствующих ключей.
- **Компрометация ключевой информации** - утрата, хищение, несанкционированное копирование или подозрение на копирование носителя ключевой информации НКИ или любые другие ситуации, при которых достоверно не известно, что произошло с НКИ. К компрометации ключевой информации также относится увольнение сотрудников, имевших доступ к ключевой информации.
- **Сертификация ключа** - процедура заверения (подписания) открытой части регистрируемого ключа электронной цифровой подписью.
- **Заявка на регистрацию ключа** - служебное сообщение, содержащее новый открытый ключ, подписанное электронной цифровой подписью.

Порядок генерации ключа:

1. Порядок генерации ЭЦП регламентируется соответствующим Регламентом Удостоверяющего центра.
2. Владельцы ЭЦП и ответственные исполнители ЭЦП назначаются приказом директора школы и действуют на основании доверенности.
3. Пользователь, обладающий правом ЭЦП (ответственный исполнитель ЭЦП), вырабатывает самостоятельно или в сопровождении администратора безопасности личный открытый ключ подписи, а также запрос на получение сертификата открытого ключа (в электронном виде и на бумажном носителе).
4. Формирование закрытых ключей подписи и шифрования производится на учтенные съемные носители информации;
5. Ни при каких обстоятельствах нельзя хранить ключи ЭЦП на жестких дисках АРМ;
6. Передавать ключи и право подписи можно исключительно по доверенности.

Порядок хранения и использования средств ЭЦП:

1. Право доступа к рабочим местам с установленным программным обеспечением средств ЭЦП предоставляется только тем лицам, которые по приказу директора школы им предоставлены полномочия на эксплуатацию этих средств.
2. Транспортирование ключевых носителей за пределы организации допускается только в случаях, связанных с производственной необходимостью. Транспортирование

ключевых носителей должно осуществляться способом, исключающим их утрату, подмену или порчу.

3. Установка пароля для доступа ЭЦП производится в соответствии с общей политикой использования паролей в школе и соответствует требованиям к паролям удостоверяющего центра.

4. При компрометации или утере ключевого носителя необходимо неотлагательно проинформировать ответственного по защите информации и представителей удостоверяющего центра.

5. На технических средствах, оснащенных средствами ЭЦП, должно использоваться только лицензионное программное обеспечение фирм-производителей.

6. Рабочие станции, на которых используется ЭЦП должны удовлетворять критериям безопасности, обозначенным в рекомендациях удостоверяющего центра.

7. Запрещается оставлять без контроля вычислительные средства, на которых эксплуатируется ЭЦП после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки.

8. Ключевая информация содержит сведения конфиденциального характера, хранится на учтенных в установленном порядке носителях и не подлежит передаче третьим лицам.

9. При необходимости временно покинуть помещение, в котором проводятся работы с использованием ЭЦП, ключевой носитель не должен быть оставлен без присмотра.

10. По факту компрометации ключей должно быть проведено служебное расследование с оформлением уведомления о компрометации.

Обязанности администратора информационной безопасности:

1. Администратор безопасности инструктирует Пользователей систем электронного документооборота по правилам обращения с ЭЦП.

2. Администратор безопасности контролирует целостность аппаратных средств и программных продуктов, используемых для систем электронного документооборота, в которых используются ЭЦП

3. Контроль за правильностью и своевременностью выполнения регламентных работ с ЭЦП осуществляет Администратор безопасности и уполномоченные лица Удостоверяющего центра.

4. Администратор безопасности осуществляет непрерывный контроль за всеми действиями Пользователей систем электронного документооборота, в которых используются ЭЦП

5. Не реже чем 2 раза в год Администратор безопасности информации проводит проверки всех АРМ пользователей, используемых для систем электронного документооборота на предмет соблюдения требований действующих Регламентов Удостоверяющих центров и настоящей Инструкции.

Обязанности ответственных исполнителей ЭЦП:

1. Ответственные исполнители ЭЦП при работе с ключевыми документами обязаны руководствоваться положениями соответствующего Регламента Удостоверяющего центра и настоящей Политики.
2. Ответственные исполнители ЭЦП обязаны организовать свою работу по генерации ЭЦП в полном соответствии с положениями соответствующего Регламента Удостоверяющего центра и настоящей Политики.
3. Ответственные исполнители ЭЦП обязаны организовать свою работу с ключевыми документами в полном соответствии с требованиями настоящего Положения.
4. Уничтожение ключевой информации с ключевого носителя может производится только в полном соответствии с положениями соответствующего Регламента Удостоверяющего центра.
5. В случае каких-либо изменений реквизитов ЭЦП (плановая смена ключей, изменение реквизитов владельцев или Ответственных исполнителей, генерация новой ЭЦП, и др.) в течение 3 суток Ответственные исполнители ЭЦП обязаны предоставить Администратору безопасности информации следующие документы:

1.1. копию Приказа о назначении Владельцев и Ответственных исполнителей ЭЦП;

1.2. копию Сертификата новой ЭЦП;

1.3. копию Акта на уничтожение ключей ЭЦП.

5. Ответственные исполнители ЭЦП обязаны выполнять требования Администратора безопасности информации в части, касающейся обеспечения информационной безопасности школы.

6.8. Использование ресурсов сети ИНТНРНЕТ

Общие положения:

1.1. Использование сети Интернет в школе направлено на решение задач учебно-воспитательного процесса.
1.2. Настоящий раздел политики информационной безопасности регулируют условия и порядок использования сети Интернет в школе;
1.3. Настоящий раздел описывает общие принципы использования сети ИНТЕРНЕТ в образовательном учреждении;
1.4. Детальные правила, нормы и регламенты использования сети ИНТЕРНЕТ определяются в положении "Об использовании сети ИНТЕРНЕТ в школе";
1.5. Требования о доступе к сети ИНТЕРНАТ, обозначенные в данном разделе, подчинены законам и иным нормативным актам РК и пересекаются с другими разделами данной политики информационной безопасности.
1.6. При использовании сети Интернет в школе обучающимся предоставляется доступ только к тем ресурсам, содержание которых не противоречит

законодательству Республики Казахстан и которые имеют прямое отношения к образовательному процессу. Проверка выполнения такого требования осуществляется с помощью специальных технических средств и программного обеспечения контентной фильтрации, установленного в школе или предоставленного оператором услуг связи.

1.7. Пользователи сети Интернет в школе должны учитывать, что технические средства и программное обеспечение не могут обеспечить гарантированную фильтрацию ресурсов сети Интернет вследствие частого обновления ресурсов. В связи с этим существует вероятность обнаружения обучающимися ресурсов, не имеющих отношения к образовательному процессу и содержание, которых противоречит законодательству Республики Казахстан. Участникам использования сети Интернет в школе следует осознавать, что школа не несет ответственности за случайный доступ к подобной информации, размещенной не на Интернет-ресурсах школы при использовании сторонних средств фильтрации содержимого контента сайтов.

1.8. Отнесение определенных ресурсов и (или) категорий ресурсов в соответствующие группы, доступ к которым регулируется техническим средствами и программным обеспечением контентной фильтрации, в соответствии с принятыми в школе Положением обеспечивается работником школы, назначенным его руководителем.

1.9. При обнаружении запрещённого содержимого после фильтрации, данная информация систематизируется и сообщается провайдеру услуги либо устраняется самостоятельно, в случае локального ограничения доступов.

1.20. Принципы размещения информации на Интернет-ресурсах школы призваны обеспечивать:

— соблюдение действующего законодательства Республики Казахстан, интересов и прав граждан;

— защиту персональных данных обучающихся, преподавателей и сотрудников;

— достоверность и корректность информации.

Использование сети ИНТЕРНЕТ в школе:

1. Использование сети Интернет в школе осуществляется, как правило, в целях образовательного процесса.

2. По разрешению лица, ответственного за организацию в школе работы сети Интернет и ограничение доступа, преподаватели, сотрудники и обучающиеся вправе:

— размещать собственную информацию в сети Интернет на Интернет-ресурсах школы;

— иметь учетную запись электронной почты на Интернет-ресурсах школы.

3. Обучающемуся запрещается:

— обращаться к ресурсам, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают законодательство Республики Казахстан (эротика, порнография, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности);
— осуществлять любые сделки через Интернет;
— осуществлять загрузки файлов на компьютер школы без специального разрешения;
— распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.
4. При случайном обнаружении ресурса, содержание которого не имеет отношения к образовательному процессу, обучающийся обязан незамедлительно сообщить об этом преподавателю, проводящему занятие. Преподаватель обязан зафиксировать доменный адрес ресурса и время его обнаружения и сообщить об этом лицу, ответственному за работу локальной сети и ограничение доступа к информационным ресурсам.

Ответственный обязан:

— принять информацию от пользователя;

— направить информацию о некатегоризированном ресурсе оператору технических средств и программного обеспечения технического ограничения доступа к информации (в течение суток);
— в случае явного нарушения обнаруженным ресурсом законодательства Республики Казахстан сообщить о нем по специальной «горячей линии» для принятия мер в соответствии с законодательством Республики Казахстан (в течение суток).

Передаваемая информация должна содержать:

— доменный адрес ресурса;

— сообщение о тематике ресурса, предположения о нарушении ресурсом законодательства Республики Казахстан либо его несовместимости с задачами образовательного процесса;
— дату и время обнаружения;

— информацию об установленных в школе технических средствах технического ограничения доступа к информации.

Подробный регламент использования сети Интернет работниками и обучающимися школы строиться на основании существующего положения «Об использовании сети Интернет в школе» в соответствии требованиям нормативной базы РК.

7. Общее управление системой информационной безопасности

Управление ИБ школы включает в себя:

- разработку и поддержание в актуальном состоянии Политики информационной безопасности;
- разработку и поддержание в актуальном состоянии нормативно-методических документов по обеспечению ИБ;
- обеспечение бесперебойного функционирования комплекса средств ИБ;
- осуществление контроля (мониторинга) функционирования системы ИБ;
- оценку рисков, связанных с нарушениями ИБ.

8. Реализация политики информационной безопасности

Реализация Политики ИБ школы осуществляется на основании документов, регламентирующих отдельные процедуры и процессы профессиональной деятельности в управлении.

9. Порядок внесения изменений и дополнений в политику информационной безопасности

Внесение изменений и дополнений в Политику информационной безопасности производится не реже одного раза в три года с целью приведения в соответствие определенных Политикой защитных мер реальным жизненным условиям и текущим требованиям к защите информации.

10. Контроль за соблюдением политики информационной безопасности

1. Текущий контроль за соблюдением выполнения требований Политики информационной безопасности школы возлагается на сотрудника, назначенного приказом директора школы.

2. Директор школы на регулярной основе рассматривает реализацию и соблюдение отдельных положений Политики информационной безопасности, а также осуществляет последующий контроль за соблюдением ее требований.