**УТВЕРЖДАЮ**
И.о. директора КГУ «Общеобразовательная школа имени Абая отдела образования города Костаная» Управления образования Костанайской области
_____ Бекентаев Ж.К.
«_31_» _октября_ 2023 г.

# Политика информационной безопасности КГУ «Общеобразовательная школа имени Абая отдела образования города Костаная»

на 13 листах

**РАЗРАБОТАНО**
Заместителем директора по ИКТ Храмей И.С.
КГУ «Общеобразовательная школа имени Абая отдела образования города Костаная» Управления образования Костанайской области
«_31_» _октября_ 2023 г.

г. Костанай, 2023 г.

## 1. Правила использования интернета и электронной почты

### Термины и определения

В данных Правилах аиспользуются следующие основные понятия и термины:

1) Электронные информационные ресурсы - информация, хранимая в электронном виде (информационные базы данных), содержащаяся в информационных системах;

2) Информационная система (далее - ИС) - система, предназначенная для хранения, обработки, поиска, распространения, передачи и предоставления информации с применением аппаратно-программного комплекса.

3) Интернет ресурс - электронный информационный ресурс, технология его ведения и (или) использования, функционирующие и открытой информационно-коммуникационной сети, а также организационная структура, обеспечивающая информационное взаимодействие;

4) Интернет-провайдер - организация, предоставляющая услуги доступа к Интернету и иные, связанные с Интернет услугой;

5) Рабочая станция - комплекс аппаратных и программных средств, предназначенных для решения определенного круга задач;

6) Конфиденциальная информация - информация, не содержащая государственных секретов, доступ к которой ограничен в соответствии с законами Республики Казахстан или их собственником, или владельцем в случаях, предусмотренных законодательством Республики Казахстан;

7) Мониторинг электронной почты — отслеживание электронных сообщений (куда, откуда, размер сообщений) в целях предотвращения спама, наличия вредоносного кода, которые могут передаваться с помощью электронных средств связи и защиты от него;

8) Мониторинг интернет-ресурсов - выявление тематики, посещаемых пользователями сайтов, выявление места доступа в Интернет, при этом, осуществляется только просмотр названия Интернет-ресурса (адрес сайта) в целях блокирования вредоносных сайтов;

9) Мониторинг информационной системы - применяется для проверки эффективности принятых средств контроля и проверки соответствия модели политики доступа;

10) Рассылка электронной почты - средство массовой коммуникации, группового общения и рекламы;

11) IT специалисты- ответственные за обеспечение развития и устранения сложных неисправностей в информационных системах школы, а также технической поддержке информационных ресурсов и систем.

### Назначение документа

1. Настоящие Правила по использованию электронной почты и служб Интернет на рабочих станциях школы регламентирует правила работы с электронной

почтой и службой Интернет.

2. Эффективность управления доступа к Интернету, выполнение требований к организации информационной безопасности в использовании Интернет-ресурсов контролируется структурным подразделением по обеспечению информационной безопасности.

3. Аппаратное и программное обеспечение для организации доступа в сеть Интернет и системы электронной почты принадлежит школе. Все сообщения, материалы, созданные, переданные или полученные с помощью системы электронной почты и Интернет, а также другими информационными ресурсами школы, являются и остаются собственностью школы и не могут быть личной собственностью ни одного из сотрудников.

4. Всем лицам запрещается несанкционированный просмотр сообщений и информации пользователей.

5. Использование сотрудником информационных ресурсов означает его согласие с условиями предоставления данных ресурсов.

6. Содержание информации может быть доведено до сведения уполномоченных лиц по решению руководства школы.

7. IT-специалисты, отвечающие за информационную безопасность школы имеют право блокировать вредоносные ресурсы Интернет.

8. Доступ к внешним почтовым Интернет-ресурсам запрещен.

## Обеспечение информационной безопасности

**1. При использовании электронной почты и служб Интернет запрещается:**

1) использовать ресурсы для агитации или рекламы коммерческих предприятий, пропаганды религиозных или политических идей, иных целей, не связанных, с выполнением служебных обязанностей;

2) создавать оскорбительные или провокационные сообщения. Таковыми считаются сообщения, содержащие сексуальные домогательства, расовые оскорбления, дискриминацию по половому признаку или другие комментарии, затрагивающие в оскорбительной форме вопросы возраста или сексуальной ориентации, религиозные или политические пристрастия, национальность или состояние здоровья, а также другую информацию, запрещенную законодательством Республики Казахстан;

3) использовать вложения графических, видео, исполняемых и т.п. файлов, не относящиеся к служебной деятельности, а также файлов, размер которых превышает установленный;

4) запрашивать отправлять сообщения, содержащие сведения составляющие служебную и/или конфиденциальную информацию с ограниченным доступом и/или распространением в открытом (незашифрованном с использованием государственных

шифровальных средств - средств криптографической защиты информации (СКЗИ) виде, а также с использованием зарубежных почтовых серверов;

5) пользоваться групповой рассылкой в личных целях;

6) использовать ресурсы для рассылки писем-пирамид, писем счастья, сообщений рекламного характера и другой подобной информации, не имеющей отношения к служебной деятельности;

7) распространять вредоносные файлы и программы, а также программное обеспечение и материалы, защищенные авторским правом;

8) использовать учетные записи других почтовых систем и пользователей; получать доступ к электронным сообщениям других пользователей (за исключением случаев, санкционированных руководством школы;

**При использовании Интернет запрещается:**

1) использовать Интернет в целях передачи и распространения материалов, содержащих конфиденциальную информацию с ограниченным доступом и/или распространением в открытом (незашифрованном с использованием государственных шифровальных средств - средств криптографической защиты информации (СКЗИ);

2) посещать веб-сайты, содержащие материалы террористической, экстремисткой, антиконституционной и иной деструктивной направленности;

3) посещать сомнительные и вредоносные сайты, а также сайты, информация на которых не связана с исполнением функциональных обязанностей;

4) загружать (передавать) вредоносные файлы и программы, программное обеспечение и материалы, защищенные авторским правом, а также мультимедийные файлы всех типов;

5) использовать службы Интернет-чатов;

6) устанавливать на рабочие станции, программы для работы через удаленный доступ с выходом в интернет;

7) осуществлять подключение компьютеров школы к сети Интернет через сторонних Интернет - провайдеров, а также использовать несанкционированное модемное подключение.

## 2. Правила организации процедуры аутентификации

### Общие положения

Настоящие Правила организации процедуры аутентификации (далее - Правила) определяют требования к регистрации учетных записей пользователей и парольной защиты информационных систем и предназначены для минимизации ущерба от реализации угроз информационной безопасности, а также для повышения общего уровня конфиденциальности, целостности и доступности информации в ИС школы.

1. Термины, использованные в настоящем документе, имеют следующие определения:

1) информационная безопасность (далее - ИБ) - комплекс правовых,

технических, и организационных мероприятий, направленных на обеспечение защиты информационных ресурсов от несанкционированного доступа, преднамеренного или случайного искажения и разрушения, физического разрушения, в том числе в результате воздействий техногенного и природного характера, а также состояние защищенности государственных информационных ресурсов и систем, обеспечение конфиденциальности, целостности и доступности информации;

2) информационная система (далее - ИС) – организационно - упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующая определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач.

3) Системный администратор- специалист, ответственный за администрирование, сопровождение и обеспечение бесперебойного функционирования всего комплекса ИС школы;

4) Пользователи ИС школы - сотрудники, работающие с ИС школы;

5) Конфиденциальность информации - обеспечение предоставления информации только авторизованным лицам;

6) Целостность информации - состояние информации (ресурсов автоматизированной информационной системы), при котором ее (их) изменение осуществляется только преднамеренно субъектами, имеющими на него право;

7) Аутентификация - подтверждение подлинности субъекта или объекта доступа путем определения соответствия предъявленных реквизитов доступа реализованными в системе;

8) Первичный пароль — комбинация символов (буквы, цифры, специальные символы), устанавливаемые администратором ОС, СУБД, ППО при создании новой учетной записи;

9) Основной пароль - комбинация символов (буквы, цифры, специальные символы), известная только системному администратору, используемая для подтверждения подлинности владельца учетной записи;

10) Учетная запись информация о пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в ИС школы.

**Требования к администраторам и пользователям ИС школы**

1. Администраторы и пользователи ИС школы обязаны:

1) Запомнить свой пароль, и ни в каком виде не сохранять и не передавать другим лицам;

2) Быть обязательно зарегистрированными в доменной службе школы.

3) В случае утраты или компрометации пароля должен незамедлительно оповестить непосредственнее руководство о данном факте и провести смену пароля;

4) Необходимо производить смену пароля не реже чем один раз в месяц;

5) При смене пароля, соблюдать требования согласно Приложению 1;

6) При вводе пароля исключить возможность его подсматривания

посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете и тп.) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерам и т.п.);

7) Обеспечить конфиденциальность и сохранность логина и пароля.

**Администраторы и пользователи ИС школы не имеют право:**

1) Работать под чужой учетной записью. В случае, если руководитель пользователя ИС школы предлагает пользователю ИС школы работать в таких условиях, пользователь ИС школы вправе потребовать письменного указания (приказа) руководителя и не приступать к работе до получения такого указания (приказа);

2) Подключать средства вычислительной техники в корпоративную сеть школы без регистрации его в доменной службе школы.

3) Сообщать кому-либо личный пароль;

4) Записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

5) Включать пароли в сценарии автоматического входа в систему, например, в макросы или функциональные клавиши.

+

**Требования к элементам регистрации и паролям**

1. Для работы в ИС школы необходимо иметь учетную запись пользователя ИС школы (логин и пароль).

2. При создании новой учетной записи системный администратор создает ее с первичным паролем и пользователю по электронной почте сообщает идентификатор временный пароль. При первом входе в систему пользователь обязан произвести смену временного пароля, При выборе пароля необходимо руководствоваться «Требования к паролям» (Приложение 1).

3. Владелец несет персональную ответственность за сохранение о тайне основного пароля. Запрещается сообщать пароль другим лицам, в том числе сотрудникам школы, записывать его, а также пересылать открытым текстом в электронных сообщениях.

4. Пароль никогда не следует хранить в компьютерной системе в незащищенной форме. Владелец должен избегать делать записи (например, на бумаге, в файлах, программного обеспечения или портативном устройстве) паролей, без гарантии их безопасного хранения и утверждения метода хранения.

5. Контроль блокирования учетных записей осуществляется руководителем, осуществляющего администрирование ИС школы, в соответствии с записями журнала регистрации учетных записей.

6. Ответственный сотрудник за системно-техническое обслуживание компьютеров, а также иной оргтехники на нейтральном аппарате школы, должен

обеспечить обязательную регистрацию всех пользователей школы в доменной службе школы согласно построенным правилам домена школы.

7. Политика доменной службы школы регулируется ответственным сотрудником за обеспечение информационной безопасности школы.

## Порядок смены паролей

1. Пользователь/системный администратор должен сменить основной пароль не реже чем один раз в месяц в соответствии с Приложением.
2. Основной пароль может быть создан только самим пользователем/администратором ИС
3. Школа запрещает генерировать пароли компьютерными программами и сторонними лицами.
4. Внеплановая смена основное пароля пользователем/системным администратором может быть произведена в любой момент по требованию ответственных лиц на ИБ.

## Управление паролями в ИС школы

1. Пароли являются основным средством подтверждения полномочий доступа пользователя к ИС школы. ИС школы должна предоставлять эффективное интерактивное средство обеспечения надежных паролей (Приложение 1).
2. При Управлении паролями в ИС должен быть реализован следующий функционал:
   1) Требование смены первичного пароля при первом входе и систему;
   2) Выбор и изменение паролей с процедурой их подтверждения для исключения ошибок при наборе (при необходимости);
   3) Проверки надежности паролей в соответствии с Приложением 1;
   4) Обязательная смена паролей с заданной периодичностью,
   5) Исключение использования трех последних паролей;
   6) Исключение возможность использования пароля, отличающегося от предыдущих трех последних паролей менее чем в 4 позициях;
   7) Хранить пароли в зашифрованном виде;
   8) Не выводить пароли на экран при их наборе на клавиатуре;

## Ответственность

1. В случае нарушения требований настоящего положения Правил, системный администратор привлекается к административной или иной ответственности в соответствии с действующим законодательством Республики Казахстан.
2. За разглашение парольной информации, которая представляет служебную тайну. работник привлекается к дисциплинарной ответственности в соответствии с действующим законодательством РК и внутренними нормативными актами.

## 3. Правила организации антивирусного контроля

### Общие положения

Настоящие правила предназначены для организации порядка проведения антивирусного контроля и предотвращения возникновения фактов заражения программного обеспечения и информационных систем компьютерными вирусами.

Правила регламентируют действия пользователей при организации антивирусной защиты электронных технологий школы.

### Установка и обновление антивирусных средств

1. К применению в школе допускаются только лицензионные антивирусные средства.
2. Установку и обновление антивирусных средств осуществляется подразделением, осуществляющим на договорных отношениях сервисное обслуживание информационных систем.

### Порядок проведения антивирусного контроля

1. Установка (изменение) системного и прикладного обеспечения компьютеров и локальной вычислительной сети осуществляется только в присутствии специалиста.
2. Устанавливаемое (изменяемое) на компьютер программное обеспечение проверяется на отсутствие компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера выполняется антивирусная проверка сотрудником Обслуживающей организации (далее - ОО), установившем программное обеспечение.
3. Обязательному антивирусному контролю подлежит любая информация (тестовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая к передаваемая по телекоммуникационным каналам, а также информаций со съемных носителей (магнитные диски, ленты: CD-ROM, FlashUSB, и т.п.), получаемых от сторонних лиц и организаций.
4. Пользователь осуществляет контроль за целевым использованием автоматизированного рабочего места, а также всех его внешних устройств.
5. Все программное обеспечение, устанавливаемое на защищаемые компьютеры, предварительно проверяется на наличие вредоносных программ. Контроль информации на съемных носителях производится непосредственно перед ее использованием.
6. Не реже одного раза в месяц проводится полная проверка всех файлов, хранящихся на жестких дисках защищаемого компьютера.
7. Внеочередной антивирусный контроль всех дисков и файлов защищаемого компьютера выполняется:
   - сразу после установки или изменения ПО;
   - после подключения автономного компьютера к локальной сети;

- при возникновении подозрения на наличие вредоносных программ (нетипичная работа программ, появление графических и звуковых эффектов, искажение данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).

8. В сомнительных случаях для определения факта наличия или отсутствия вредоносных программ к проверке необходимо привлечь специалистов технической поддержки.

9. Пользователям запрещается установка нелицензированного программного обеспечения на рабочие станции, самостоятельного внесения изменений в настройки конфигурации, а также отключение, удаление антивирусных программ.

### Действия сотрудников при обнаружении компьютерного вируса

1. При возникновении подозрения на наличие компьютерного вируса сотрудник школы проводит внеочередной антивирусный контроль или при необходимости привлекает it-специалиста для определения ими факта наличия или отсутствия компьютерного вируса.

2. При обнаружении компьютерного вируса сотрудник школы обязан приостановить работу, поставить в известность о факте обнаружения зараженных вирусом файлов сотрудников, осуществляющих техническое обслуживание;

### Контроль при организации антивирусной защиты

1. Контроль за организацией антивирусной зашиты в школе и установление порядка её поведения возлагается на сотрудников, обеспечивающих информационную безопасность (администрирование антивирусной системы защиты, системы обеспечения адаптивной безопасности и т.д.).

2. Периодический контроль за соблюдением положений данной инструкции возлагается на заместителя директора по ИКТ.

### Организация антивирусной зашиты

1. Пользователь обязан регулярно проверять антивирусную базу.

2. При отсутствии антивирусной программы немедленно сообщить сотрудникам, отвечающим за информационную безопасность.

## 4 Инструкции о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях

### Общие положения и основные понятия

Настоящая Инструкция о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях определяет основные меры, методы и средства сохранения (поддержания) работоспособности информационных систем (далее КС) при возникновении различных кризисных ситуаций, а также

способы и средства восстановления информации и процессов ее обработки в случае нарушения работоспособности ИС и ее основных компонентов. Кроме того, она описывает действия различных категорий персонала системы в кризисных ситуациях по ликвидации их последствий и минимизации наносимого ущерба.

1. Ситуация, возникающая в результате нежелательного воздействия на ИС, приведшая к угрозе информационной безопасности, называется кризисной. Кризисная ситуация может возникнуть в результате преднамеренных действий злоумышленника или непреднамеренных действий пользователей, аварий, стихийных бедствий.

2. По степени серьезности и размерам наносимого ущерба кризисные ситуации разделяются на следующие категории:

1) угрожающая - приводящая к полному выходу из строя ИС и неспособности выполнять далее свои функции, а также к уничтожению, блокированию, неправомерной модификации или компрометации наиболее важной информации.

3. К угрожающим кризисным ситуациям относятся:

1) нарушение подачи электроэнергии в здании;

2) выход из строя рабочей станции, отвечающей за файловый обмен (с потерей информации);

3) выход из строя рабочей станции, отвечающей за файловый обмен (без потери информации),

4) частичная потеря информации на рабочей станции, отвечающей за файловый обмен, без потери его работоспособности;

5) выход из строя локальной сети (физической среды передачи данных);

6) серьезная - приводящая к выходу из строя отдельных компонентов системы (частичной потере работоспособности), потере производительности, а также к нарушению целостности и конфиденциальности программ и данных в результате несанкционированного доступа.

4. К серьезным кризисным ситуациям относятся:

1) выход из строя рабочей станции (с потерей информации);

2) выход из строя рабочей станции (без потери информации);

3) частичная потеря информации на рабочей станции без потери ее работоспособности;

4) стихийные бедствия (пожар, наводнение, ураган и т.д.).

5. Подробное описание о порядке действий пользований во внештатных (кризисных) ситуациях находится в Приложении 1 к данной Политики безопасности.

6. Источники Информации о возникновении кризисной ситуации:

1) пользователи, обнаружившие подозрительные изменения в работе или конфигурации системы, или средств ее защиты в своей зоне ответственности;

2) средства защиты, обнаружившие кризисную ситуацию;

3) системные журналы, в которых имеются записи, свидетельствующие о возникновении или возможности возникновения кризисной ситуации.

## Общие требования

1. Все пользователи, работа которых нарушена в результате возникновения угрожающей или серьезной кризисной ситуации, немедленно оповещаются посредством электронной почты администраторами ИС. Дальнейшие действия по устранению причин нарушения работоспособности ИС, возобновлению обработки и восстановлению поврежденных (утраченных) ресурсов определяются функциональными обязанностями персонала и пользователей системы.

2. Каждая кризисная ситуация анализируется ОИ. По результатам этого анализа вырабатываются предложения по изменению полномочий пользователей, атрибутов доступа к ресурсам, созданию дополнительных резервов по изменению конфигурации системы или параметров настройки средств защиты и т.п., при необходимости приводится расследование причин ее возникновения, оценка причинного ущерба, определение виновных и принятие соответствующих мер.

3. Серьезная и угрожающая кризисная ситуация требует оперативной замены и ремонта вышедшего из строя оборудования, а также восстановления поврежденных программ и наборов данных из резервных копий.

4. Оперативное восстановление программ (используя эталонные копии) и данных (используя страховые копии) в случае их уничтожения или порчи с серьезной или угрожающей кризисной ситуации обеспечивается резервным (страховым) копированием и внешним (по отношению к основным компонентам системы) хранения копий. Внешнее хранение подразумевает нахождение копий в выделенных хранилищах (сейфах), находящихся в специально отведенных помещениях.

5. Резервному копированию подлежат все программы и данные, обеспечивающие работоспособность и выполнение задач системы (системное и прикладное программное обеспечение, открытых данных и другие наборы данных), а также архивы, журналы транзакций, системные журналы и т.д.

6. Все программные средства, используемые в системе, имеют эталонные (дистрибутивные) копии.

7. Необходимые действия персонала по созданию, хранению и использованию резервных копий программ и данных отражаются в функциональных обязанностях соответствующих категорий персонала, как правило это - Системные администраторы, администраторы автоматизированных рабочих мест, сотрудники ОИ, а также фиксируются в реестре.

8. Обязанности и действия персонала по обеспечению непрерывной работы и восстановлению информационных систем.

9. Действия персонала в кризисной ситуации зависят от степени ее тяжести.

10. В случае возникновения угрожающей или серьезной критической ситуации действия персонала включают следующие этапы:

1) немедленная реакция ответственного персонала;

11. В кризисных (внештатных) ситуациях пользователи немедленно оповещаются посредством внутренней электронной почты, устно по телефону или с

помощью электронных средств связи сотрудниками Обслуживающей организации (далее - ОО), ОИ.

12. В дневное время суток пользователь, обнаруживший внештатную (кризисную) ситуацию, ставит в известность сотрудников ОО, СА в части технической поддержки информационных ресурсов и систем.

13. В ночное время суток, при возникновении внештатной ситуации обнаруживший пользователь должен поставить в известность сотрудника ОИ, и срочном порядке средствами телефонной связи оповещаются: ответственные руководители структурных подразделений за данный участок работ, руководство ОИ. Событие в обязательном порядке регистрируется в журнале, с указанием точного времени инцидента, краткого описания событий, с указанием Ф.И.О. оповещенных руководителей структурных подразделений, описания действий, направленных на устранение кризисной ситуации.

1) частичное восстановление работоспособности и возобновление обработки;

2) полное восстановление системы и возобновление обработки в полном объеме;

3) расследование причин возникновения кризисной ситуации и установление виновных;

4) выработка решений по устранению причин и недопущения в последующем подобных фактов нарушений.

14. Контроль за организацией работ в кризисных ситуациях осуществляет ДЦ.

**Использование удаленного доступа**

Запретить установку программ для работы через удаленный доступ на рабочих станциях с выходом в интернет.

**Использования флеш-карт**

В связи со служебной необходимостью разрешить использование *флеш-карт (E-token, KAZ-token, Save-Token, Usb-носителей)* в компьютерах, предназначенных для сотрудников бухгалтерии, административного состава, учителей, социальных педагогов.