УТВЕРЖДЕНА

приказом и.о. директора

МАОУ «Школа-интернат № 85»

г.Перми

от 16.11.2017 № СЭД-059-01-12-89

**ПОЛИТИКА**

**информационной безопасности**

**МАОУ «Школа-интернат № 85» г.Перми**

1. **Общие положения**
   1. Настоящая Политика информационной безопасности МАОУ «Школа-интернат №85» г. Перми (далее – Политика ИБ) разработана в целях установления безопасных способов обработки информации в электронном виде, в том числе в информационных системах (сайтах).
   2. Настоявшая Политика ИБ определяет цели и задачи защиты информации, устанавливает методы защиты информации, которыми должны руководствоваться работники при обработке информации в электронном виде, в том числе в информационных системах (сайтах).
   3. Настоящая Политика ИБ применима ко всем техническим средствам (серверу, периферийному оборудованию, автоматизированным рабочим местам (далее – АРМ и т.д.), установленных в МАОУ «Школа-интернат №85» г. Перми, ко всем процессам обработки информации с использованием указанных технических средств.
   4. Правовыми основаниями настоящей Политики ИБ являются Конституция Российской Федерации, Гражданский кодекс Российской Федерации, Уголовный кодекс Российской Федерации, Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. **Термины и определения**

В настоящей политике ИБ используются следующие термины и определения:

В настоящей Политике ИБ используются следующие термины и определе­ния:

вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкциониро­ванного распространения и самовоспроизведения;

вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных;

доступность информации - состояние информации, при котором субъекты, имеющие санкционированные права доступа, могут реализовать их беспрепят­ственно;

защищаемая информация - информация, являющаяся предметом собствен­ности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

идентификатор (имя, логин) - набор символов, представляющий уникаль­ное наименование объекта или субъекта в информационной системе, позволяю­щее однозначно идентифицировать пользователя при входе его в систему, опре­делить его права в ней, фиксировать действия и тому подобное;

информационная безопасность - состояние защищенности информационной среды;

информационная среда - совокупность условий для технологической пере­работки и эффективного использования информационных ресурсов (в том числе технические средства, программное обеспечение, телекоммуникации, уровень подготовки пользователей, формы контроля, документопотоки, процедуры, ре­гламенты, юридические нормы, иные факторы, воздействующие на информаци­онные процессы и информационные системы);

информационные ресурсы - отдельные документы, массивы документов, в том числе содержащиеся в информационных системах (архивах, фондах, банках данных, других информационных системах);

инцидент информационной безопасности - любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информаци­онную безопасность;

несанкционированное действие - действие субъекта в нарушение установ­ленных в информационной системе регламентируемых правил обработки инфор­мации;

оператор информационной системы администрации города Перми (далее - оператор информационной системы) - функциональный, территориальный орган или функциональное подразделение администрации города Перми, определяю­щий цели и порядок эксплуатации информационной системы;

пароль - конфиденциальная последовательность символов, связанная с субъектом и известная только ему, позволяющая его аутентифицировать, то есть подтвердить соответствие реальной сущности субъекта предъявляемому им при входе идентификатору;

профиль - набор установок и конфигураций, специфичный для данного субъекта или объекта и определяющий его работу в информационной системе;

системный администратор - лицо, обеспечивающее выполнение функций по обеспечению работы компьютерной техники, сети и программного обеспече­ния в функциональном, территориальном органе, функциональном подразделении администрации города Перми. Для функциональных подразделений администра­ции города Перми функции системного администратора выполняют специалисты управления информационных технологий администрации города Перми (далее - УИТ);

угроза безопасности информации - потенциально возможное событие, дей­ствие, процесс или явление, которое может привести к нарушению конфиденци­альности, целостности, доступности информации, а также неправомерному тира­жированию, которое наносит ущерб собственнику, владельцу или пользователю информации;

уязвимость - свойство информационной системы, обусловливающее возможность реализации угроз безопасности, обрабатываемой в ней информации;

целостность информации - состояние информации, при котором отсутству­ет любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими санкционированное право на изменение информации.

Термины «информация, информационная система, информационная систе­ма персональных данных, конфиденциальность информации, обладатель инфор­мации, сайт в сети Интернет (далее - сайт), спам, обезличивание персональных данных, общедоступная информация» используются в значениях, установленных Федеральными законами от 27 июля 2006 г. № 149-ФЗ «Об информации, инфор­мационных технологиях и о защите информации», от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федера­ции от 10 сентября 2007 г. № 575 «Об утверждении Правил оказания телематиче­ских услуг связи».

1. **Цели и задачи защиты информации в МАОУ «Школа-интернат №85» г. Перми, основные виды угроз безопасности информации**
   1. Обеспечение информационной безопасности в МАОУ «Школа-интернат №85» г. Перми – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и (или) непреднамеренных воздействий на защищаемую информацию, ее носители, процессы обработки.
   2. Защищаемой информацией является информация, обрабатываемая в МАОУ «Школа-интернат №85» г. Перми независимо от ее местонахождения в информационной среде.

Уровни конфиденциальности:

- общедоступная (открытая) информация, для которой требуется обеспечение доступности и целостности;

- информация ограниченного распространения, для которой наравне с доступностью и целостностью требуется обеспечение конфиденциальности.

* 1. Основными задачами защиты информации являются:

- выявление и оценка потенциальных угроз информационной безопасности и уязвимостей объектов защиты;

- исключение либо минимизация выявленных угроз безопасности;

- предотвращение инцидентов информационной безопасности.

* 1. Угрозы безопасности информации могут быть реализованы за счет:

- утечки по техническим каналам;

- несанкционированного доступа с использованием соответствующего программного обеспечения.

* 1. Угрозы безопасности информации могут проявляться в виде инцидентов информационной безопасности:

- утрата информации, оборудования или устройств;

-системные сбои и перезагрузки;

- противоправные и (или) ошибочные действия сотрудников при работе на АРМ;

- нарушение правил обработки информации, в том числе разглашение паролей доступа к информационным ресурсам, которые повлекли или могли повлечь нарушение конфиденциальности, целостности и (или) доступности информации;

- нарушение физических мер защиты;

- неконтролируемые изменения систем;

- сбои программного обеспечения, отказы в обслуживании сервисов, средств обработки информации, оборудования;

- нарушение правил доступа;

- внедрение вредоносных программ.

* 1. В качестве методов защиты информации в МАОУ «Школа- интернат №85» г. Перми применяются:

- регламентация доступа в служебные помещения;

- разграничение доступа к техническим средствам и информационным ресурсам;

- применение антивирусной защиты;

- регламентация использования электронной почты;

- регламентация работы в сети Интернет;

- проведение внутреннего контроля и обучения сотрудников.

1. **Регламентация доступа в служебные помещения МАОУ «Школа – интернат №85» г. Перми**
   1. Регламентация доступа в служебные помещения МАОУ «Школа-интернат №85» г. Перми осуществляется в целях:

- обеспечение физической сохранности носителей информации, оборудования;

- исключение возможности несанкционированного доступа в служебные помещения, в том числе в которых ведется обработка конфиденциальной информации.

* 1. Доступ сотрудников и посетителей в МАОУ «Школа-интернат № 85» г.Перми осуществляется в соответствии с Положением о пропускном режиме, утвержденным приказом директора школы - интерната от 27.10.2015 № СЭД-01-08-93.

1. **Разграничение доступа к техническим средствам и информационным ресурсам**
   1. Разграничение доступа к техническим средствам и информационным ресурсам направлено на предотвращение получения информации, обрабатываемой в электронном виде, в том числе в информационных системах, с нарушением регламентируемых нормативными правовыми актами или владельцами информации правил, следствием которых может быть нарушение конфиденциальности, целостности и (или) доступности информации.
   2. Для работы с информационными ресурсами работникам МАОУ «Школа-интернат №85» г. Перми предоставляется АРМ.

ПО АРМ устанавливается и обновляется системным администратором со специальных ресурсом или съемных носителей в соответствии с лицензионным соглашением.

При передаче АРМ другому сотруднику производится удаление профиля АРМ.

* 1. К работе с информационными ресурсами допускаются сотрудники, ознакомленные с настоящей Политикой ИБ.
  2. Для осуществления доступа к информационным ресурсам сотруднику создается учетная запись – присваивается уникальный идентификатор (имя, логин) и пароль доступа;
  3. Для защиты своих паролей сотрудники обязаны:

- соблюдать конфиденциальность пароля – не сообщать пароль другим лицам, в том числе другим сотрудникам, не хранить пароли в легкодоступных местах (на столе, стене, терминале и т.д.);

- выбирать трудноугадываемый пароль – использовать в пароле строчные и прописные буквы, цифры, специальные символы, не использовать в качестве пароля свои фамилию, имя, отчество, цифровые ряды или повторяющиеся цифры (123456, 111111 и т.д.);

- использовать в пароле не менее 8 символов;

- в случае компрометации пароля немедленно изменить пароль.

* 1. При работе на АРМ сотрудники обязаны:

- работать только под своей учетной записью;

- блокировать доступ к АРМ при отсутствии на рабочем месте.

* 1. Сотрудникам запрещается самостоятельно устанавливать на АРМ дополнительные технические средства и (или) ПО.

1. **Антивирусная защита**
   1. Антивирусная защита применяется с целью защиты информационных ресурсов и ПО от несанкционированных дей­ствий (утраты, модификации, изменения) путем внедрения в информационную среду вирусов, вредоносных программ (далее - вирус) посредством использова­ния специализированного ПО (далее - антивирусное ПО).
   2. Антивирусное ПО должно быть развернуто на всех технических сред­ствах, подверженных воздействию вирусов (АРМ, серверах). Антивирусные ме­ханизмы должны быть актуальными, постоянно включенными. Должны вестись журналы протоколирования событий. Отключение антивирусного ПО или отказ от автоматического обновления антивирусных баз не допускается.
   3. Обязанность по установке и регулярному обновлению антивирусного ПО, в том числе антивирусных баз, на АРМ и серверах возлагается на соответствующих системных администраторов.
   4. При установке антивирусного ПО системным администратором должны выполняться следующие требования:

- актуализация антивирусных баз на АРМ, подключенных к локальной сети, должна осуществляться ежедневно в автоматиче­ском режиме через специальный сервер обновлений;

- актуализация антивирусных баз на АРМ, не подключенных к локальной сети, должна осуществляться с использованием съемных носителей информации не реже одного раза в неделю;

- проверка критических областей АРМ, заражение которых вирусами может привести к серьезным последствиям, должна проводиться автоматически при каждой его загрузке.

* 1. Некоторые признаки проявления вируса:

- прекращение работы или неправильная работа ранее успешно функциони­ровавшего ПО;

- медленная работа АРМ;

- невозможность загрузки операционной системы;

- нетипичная работа ПО;

- вывод на экран непредусмотренных сообщений или изображений;

- подача непредусмотренных звуковых сигналов;

- частые зависания и сбои в работе АРМ;

- частое появление сообщений о системных ошибках;

- исчезновение файлов, каталогов или искажение их содержимого;

- изменение даты и времени модификации файлов;

- изменение размеров файлов;

- неожиданное значительное увеличение количества файлов на диске; существенное уменьшение размера свободной оперативной и дисковой па­мяти.

* 1. Для исключения заражения вирусами и обеспечения надежного хране­ния информации в электронном виде сотрудники обязаны:

- убедиться, что на АРМ установлено и включено антивирусное ПО;

- незамедлительно сообщить системному администратору о нарушениях ра­боты антивирусного ПО;

- перед использованием проверять съемные носители информации на нали­чие вирусов средствами установленного на АРМ антивирусного ПО;

- при переносе на свой АРМ файлов в архивированном виде проверять их до и после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами;

- использовать антивирусное ПО для входного контроля всех файлов (испол­няемых файлов, файлов данных, сообщений электронной почты и так далее), по­лучаемых из компьютерных сетей, а также на съемных носителях информации;

- в случае установки или изменения ПО при возникновении подозрения на наличие вирусов проверять на наличие вирусов жесткие диски АРМ, запуская антивирусное ПО для тестирования файлов, памяти и системных областей дисков.

* 1. Сотрудникам запрещается:

- открывать приложения и документы в письмах, получаемых по электронной почте, если имеются сомнения в надежности отправителя и (или) отправления;

- переходить по ссылкам в спам-письмах;

- загружать файлы с сайтов, если имеются сомнения в надежности сайта и (или) загружаемого файла.

* 1. При возникновении подозрения на наличие вирусов сотрудники обязаны:

- приостановить все операции, связанные с обработкой файлов на АРМ;

- запустить антивирусное ПО для тестирования файлов, памяти и системных областей дисков;

- о факте обнаружения вирусов немедленно сообщить системному админи­стратору, владельцам зараженных или поврежденных вирусами файлов, другим пользователям, использующим зараженные файлы в работе;

- провести анализ необходимости дальнейшего использования зараженных вирусом файлов;

- провести самостоятельно или совместно с системным администратором лечение зараженных файлов, в случае обнаружения не поддающегося лечению вируса удалить инфицированный файл и проверить работоспособность компью­тера.

* 1. Сотрудники допускаются к работе на АРМ только после обучения пользованию средствами антивирусного ПО в соответствии с разделом 12 настоящей Политики ИБ.

1. **Регламентация использования электронной почты**
   1. Система электронной почты МАОУ «Школа-интернат №85» г. Перми (далее - электронная почта) используется в информационных целях, в том числе оповеще­ния, организации работы, обеспечения внутренних и внешних коммуникаций.
   2. Регламентация использования электронной почты осуществляется с це­лью снижения риска умышленной или неумышленной несанкционированной рас­сылки информации, заражения информационных ресурсов вирусами.
   3. Угрозы, связанные с электронной почтой:

- возможность создания писем с фальшивыми адресами;

- возможность нарушения конфиденциальности электронных писем;

- возможность изменения в процессе передачи содержимого электронных пи­сем;

- осуществление сетевых атак посредством отправки упакованного в архив сообщения, распаковка которого приводит к выводу системы из строя, заражения вирусами;

- получение спама.

* 1. При работе с электронной почтой секретарь обязаны:

- перед отправкой тщательно проверять сообщения на отсутствие информа­ции, указанной в пункте 9.6 настоящей Политики ИБ;

- периодически удалять из электронного почтового ящика ненужные сообще­ния и перемещать необходимые сообщения в архивные почтовые папки;

- проверять сообщения электронной почты на наличие вирусов;

- использовать шифрование, обезличивание конфиденциальной информации при ее отправке.

* 1. При работе с электронной почтой сотрудникам запрещено:

- отправлять конфиденциальную информацию без предварительного шифро­вания криптографическим ПО;

- отправлять персональные данные без предварительного обезличивания или шифрования;

- использовать электронную почту для создания, отправки, пересылки или хранения любых подрывных, оскорбительных, неэтичных, незаконных материа­лов, включая оскорбительные комментарии по поводу расы, пола, цвета, инва­лидности, возраста, сексуальной ориентации, порнографии, терроризма, религи­озных убеждений и верований, политических убеждений, национальном проис­хождении, гиперссылок или других ссылок на веб-сайты, содержащие указанные материалы, массовые рассылки спама;

- рассылать компьютерные коды, файлы или ПО, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компью­терного или телекоммуникационного оборудования, вирусы или другое злонаме­ренное ПО, программы для осуществления несанкционированного доступа, се­рийные номера к программным продуктам и программы для их генерации, логи­ны, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети Интернет, ссылки на указанную информацию;

- перехватывать, изменять, удалять, сохранять или публиковать сообщения иных сотрудников, кроме случаев, санкционированных руководителями или в целях администрирования систем;

- использовать веб-сервисы Google, Gmail, Hotmail, Yahoo, Яндекс или по­добные почтовые системы третьих сторон («вебмайл») для отправки и (или) по­лучения служебной корреспонденции;

- загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным ПО, переходить по активным ссылкам, полученным от отправителей, если имеются сомнения в надежности отправителя и (или) полученного сообщения.

* 1. Содержимое электронного почтового ящика сотрудника может быть проверено системным администратором без предварительного уведомления сотрудника в случае подозрения на осуществление рассылки писем, содержащих вре­доносное ПО, спам, информацию, распространение которой запрещено правовы­ми актами. Информация о выявленных нарушениях направляется сотруднику и руководителю учреждения.

1. **Регламентация работы в сети Интернет**
   1. Сеть Интернет в МАОУ «Школа-интернат №85» г. Перми используется сотрудниками для получения информации в рамках исполнения должностных обязанно­стей.
   2. Регламентация работы в сети Интернет осуществляется с целью сни­жения риска заражения информационных ресурсов вирусами.
   3. Доступ к сети Интернет предоставляется сотрудникам с АРМ, закреп­ленным за сотрудником для исполнения должностных обязанностей.
   4. Угрозы, связанные с работой в сети Интернет:

- легкость перехвата данных и фальсификации IP-адресов в сети Интернет;

-заражение вирусами.

* 1. Сотрудникам запрещается:

- осуществлять действия, запрещенные законодательством Российской Феде­рацией;

- отправлять конфиденциальную информацию без предварительного шифро­вания криптографическим ПО, разрешенным к использованию;

- распространять информацию, содержащую подрывные, оскорбительные, неэтичные, незаконные материалы, включая оскорбительные комментарии по по­воду расы, пола, цвета, инвалидности, возраста, сексуальной ориентации, порно­графии, терроризма, религиозных убеждений и верований, политических убежде­ний, национальном происхождении, гиперссылок или других ссылок на веб­сайты, содержащие указанные материалы, массовые рассылки спама;

- самостоятельно устанавливать на АРМ дополнительное ПО, полученное в сети Интернет;

- загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным ПО;

- открывать страницы сайтов, если имеются сомнения в надежности сайта и (или) имеются уведомления о возможном заражении вирусами.

* 1. Сотрудники обязаны при обнаружении попыток несанкционированного доступа и (или) при подозрении на наличие вируса немедленно прекратить работу в сети Интернет и сообщить системному администратору.
  2. Вся информация о ресурсах, посещаемых сотрудником, автоматически протоколируется и при необходимости представляется системным администратором руководителю.
  3. На каждом АРМ системным администратором должна быть установлена контент – фильтрация.
  4. Доступ к сети Интернет может быть блокирован системным администратором без предварительного уведомления сотрудника при возникновении угрозы безопасности информации.

1. **Проведение внутреннего контроля и обучения сотрудников**
   1. В целях выявления угроз безопасности информации, нарушений настоящей Политики ИБ и принятия мер, направленных на предотвращение угроз и нарушений, в МАОУ «Школа-интернат №85» г. Перми осуществляется внутренний контроль:
      1. использования технических средств, ПО, работы в сети Интернет;
      2. обработки персональных данных в соответствии с утвержденными распоряжением администрации города Перми от 24 августа 2012 г. № 81 Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленными Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами администрации города Перми.
   2. Ознакомление сотрудников с настоящей Политикой ИБ производится при:

- приеме на работу;

- изменении настоящей Политики ИБ;

- обнаружении действий сотрудников, которые повлекли или могли повлечь нарушение безопасности информации.

* 1. Обучение сотрудников пользованию средствами антивирусного ПО производится при:

- приеме на работу;

- изменении антивирусного ПО;

- заражении АРМ вирусами.

* 1. Ознакомление сотрудников с настоящей Политикой ИБ и обучение пользованию средствами антивирусного ПО осуществляется под подпись в листе ознакомления (прохождения обучения) либо журнале ознакомления (прохождения обучения) с указанием фамилии, имени, отчества служащего и даты ознакомления (прохождения обучения).

Обязанность по организации ознакомления сотрудников с настоящей Политикой ИБ возлагается на заместителей руководителя.

Обязанность по обучению пользованию средствами антивирусного ПО возлагается на системных администраторов.

1. **Ответственность за нарушения настоящей Политики ИБ**
   1. Сотрудники в рамках должностных обязанностей и полномочий несут ответственность в соответствии с действующим законодательством Российской Федерации за:

- невыполнение требований настоящей Политики ИБ;

- действия или бездействие, ведущие к нарушению информационной безопасности;

- действия или бездействие, ведущие к нарушению действующего законодательства Российской Федерации в области информационных технологий.

* 1. При обнаружении нарушения сотрудниками настоящей Политики ИБ системный администратор устанавливает причины возникновения нарушения и направляет служебную записку о выявленном нарушении руководителю учреждения, который принимает решение о необходимости привлечения сотрудника к ответственности.
  2. Системный администратор ведет учет всех выявленных случаев нарушения безопасности информации.