УТВЕРЖДАЮ
Директор МАОУ «СОШ №127» г.Перми
_____ Кренинг Е.А.
Приказ 059-08/116-01-37/4-122
от « 26» мая 2022 г.

Регламент
информационной безопасности МАОУ «СОШ №127» г. Перми

1.Общие положения

1.1. Настоящий Регламент информационной безопасности (далее-Регламент) МАОУ «СОШ №127» г. Перми (далее - ОУ) разработан в целях установления безопасных способов обработки информации в электронном виде, в том числе в информационных системах (сайтах) ОУ

1.2. Настоящая Регламент ИБ определяет цели и задачи защиты информации, устанавливает методы защиты информации, которыми должны руководствоваться работники МАОУ «СОШ №127» г. Перми при обработке информации в электронном виде, в том числе в информационных системах, ответственность за нарушение требований настоящей Политики ИБ.

1.3. Настоящая Политика ИБ применима ко всем техническим средствам (серверам, периферийному оборудованию, автоматизированным рабочим местам (далее - АРМ) и так далее), установленным в МАОУ «СОШ №127» г. Перми, ко всем процессам обработки информации с использованием указанных технических средств.

1.4. Правовыми основаниями настоящей Политики ИБ являются Конституция Российской Федерации, Гражданский кодекс Российской Федерации, Уголовный кодекс Российской Федерации, Кодекс Российской Федерации об административных правонарушениях, Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», иные нормативные правовые акты Российской Федерации, документы Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности, Федеральной службы по надзору в сфере связи и массовых коммуникаций.

2. Термины и определения

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

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

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

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

2.5. 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;

2.6. информационная безопасность - состояние защищенности информационной среды;
2.7. 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);
2.8. информационные ресурсы - отдельные документы, массивы документов, в том числе содержащиеся в информационных системах (архивах, фондах, банках данных, других информационных системах);
2.9. инцидент информационной безопасности -- любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность;
2.10. несанкционированное действие - действие субъекта в нарушение установленных в информационной системе регламентируемых правил обработки информации;
2.11. 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;
2.12. профиль - набор установок и конфигураций, специфичный для данного субъекта или объекта и определяющий его работу в информационной системе;
2.13. системный администратор - лицо, обеспечивающее выполнение функций по обеспечению работы компьютерной техники, сети и программного обеспечения в образовательном учреждении;
2.14. 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;
2.15. уязвимость - свойство информационной системы, обусловливающее возможность реализации угроз безопасности, обрабатываемой в ней информации;
2.16. целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими санкционированное право на изменение информации.
2.17. 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».

3. Цели и задачи защиты информации в ОУ, основные виды угроз безопасности информации

3.1. Обеспечение информационной безопасности в образовательном учреждении (защита информации) - деятельность, направленная на предотвращение утечки защищаемой информации, - несанкционированных и (или) непреднамеренных воздействий на защищаемую информацию, ее носители, процессы обработки.

3.2. Защищаемой информацией в образовательном учреждении является вся информация, обрабатываемая в образовательном учреждении (далее – информация), независимо от ее местонахождения в информационной среде.
3.3. В ОУ обрабатывается информация различных уровней конфиденциальности:
3.3.1. общедоступная (открытая) информация, для которой требуется обеспечение доступности и целостности;
3.3.2. информация ограниченного распространения, доступ к которой ограничивается в соответствии с действующим законодательством Российской Федерации (далее - конфиденциальная информация), и наравне с доступностью и целостностью требуется обеспечение конфиденциальности.
3.4. Уровень конфиденциальности устанавливается обладателем информации.
3.5. Основными задачами защиты информации в образовательном учреждении являются:
3.5.1. выявление и оценка потенциальных угроз информационной безопасности и уязвимостей объектов защиты;
3.5.2. исключение либо минимизация выявленных угроз безопасности;
3.5.3. предотвращение инцидентов информационной безопасности.
3.6. Угрозы безопасности информации могут быть реализованы за счет:
3.6.1. утечки по техническим каналам утечки информации;
3.6.2. несанкционированного доступа с использованием соответствующего программного обеспечения.
3.7. Угрозы безопасности информации могут проявляться в виде инцидентов информационной безопасности:
3.7.1. утрата информации, оборудования или устройств;
3.7.2. системные сбои или перегрузки;
3.7.3. противоправные и (или) ошибочные действия работников при работе на АРМ;
3.7.4. 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;
3.7.5. нарушение физических мер защиты;
3.7.6. неконтролируемые изменения систем;
3.7.7. сбои программного обеспечения, отказы в обслуживании сервисов, средств обработки информации, оборудования;
3.7.8. нарушение правил доступа;
3.7.9. внедрение вредоносных программ.

4. В качестве методов защиты информации в ОУ применяются:

4.1.1. регламентация доступа в служебные помещения ОУ (положение об охране);
4.1.2. разграничение доступа к техническим средствам и информационным ресурсам ОУ;
4.1.3. применение антивирусной защиты;
4.1.4. применение криптографической защиты информации;
4.1.5. применение обезличивания персональных данных;
4.1.6. регламентация использования электронной почты;
4.1.7. регламентация работы в сети Интернет;
4.1.8. регламентация создания и эксплуатации информационных систем;
4.1.9. проведение внутреннего контроля и обучение работников.

5. Порядок работы с информационными ресурсами

5.1. Для работы с информационными ресурсами ОУ служащему предоставляется АРМ. ПО АРМ устанавливается и обновляется системным администратором со специальных ресурсов или съемных носителей в соответствии с лицензионным соглашением. При

прекращении полномочий пользователя производится удаление профиля пользователя АРМ.
5.2. К работе с информационными ресурсами ОУ допускаются работники, ознакомленные с настоящей Политикой ИБ.
5.3. Для осуществления доступа к информационным ресурсам ОУ служащему создается учетная запись - присваивается уникальный идентификатор (имя, логин) и пароль доступа.
5.4. Для защиты своих паролей работники обязаны:
5.4.1. соблюдать конфиденциальность пароля - не сообщать пароль другим лицам, в том числе другим работникам, не хранить пароли в легкодоступных местах (на столе, стене, терминале и так далее);
5.4.2. в случае компрометации пароля немедленно сообщить об этом системному администратору и запросить новый пароль.
5.5. При работе на АРМ работники обязаны:
5.5.1. работать только под своей учетной записью;
5.5.2. блокировать доступ к АРМ при отсутствии на рабочем месте.
5.6. Работникам запрещается самостоятельно устанавливать на АРМ дополнительные технические средства и (или) ПО.

6. Антивирусная защита

6.1. Антивирусная защита в ОУ 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).
6.2. 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.
6.3. Обязанность по установке и регулярному обновлению антивирусного ПО, в том числе антивирусных баз, на АРМ и серверах ОУ возлагается на соответствующих системных администраторов.
6.4. При установке антивирусного ПО системным администратором должны выполняться следующие требования:
6.4.1. актуализация антивирусных баз на АРМ, подключенных к локальной сети ОУ, должна осуществляться ежедневно в автоматическом режиме через специальный сервер обновлений;
6.4.2. проверка критических областей АРМ, заражение которых вирусами может привести к серьезным последствиям, должна проводиться автоматически при каждой его загрузке.
6.5. Некоторые признаки проявления вируса:
6.5.1. прекращение работы или неправильная работа ранее успешно функционировавшего ПО;
6.5.2. медленная работа АРМ;
6.5.3. невозможность загрузки операционной системы;
6.5.4. нетипичная работа ПО;
6.5.5. вывод на экран непредусмотренных сообщений или изображений;
6.5.6. подача непредусмотренных звуковых сигналов;
6.5.7. частые зависания и сбои в работе АРМ;
6.5.8. частое появление сообщений о системных ошибках;

6.5.9. исчезновение файлов, каталогов или искажение их содержимого;
6.5.10. изменение даты и времени модификации файлов;
6.5.11. изменение размеров файлов;
6.5.12. неожиданное значительное увеличение количества файлов на диске;
6.5.13. существенное уменьшение размера свободной оперативной и дисковой памяти.
6.6. Для исключения заражения вирусами и обеспечения надежного хранения информации в электронном виде работники обязаны:
6.6.1. убедиться, что на АРМ установлено и включено антивирусное ПО;
6.6.2. незамедлительно сообщить системному администратору о нарушениях работы антивирусного ПО;
6.6.3. перед использованием проверять съемные носители информации на наличие вирусов средствами установленного на АРМ антивирусного ПО;
6.6.4. 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;
6.6.5. 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;
6.6.6. 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.
6.7. Работникам запрещается:
6.7.1. открывать приложения и документы в письмах, получаемых по электронной почте, если имеются сомнения в надежности отправителя и (или) отправления;
6.7.2. переходить по ссылкам в спам-письмах;
6.7.3. загружать файлы с сайтов, если имеются сомнения в надежности сайта и (или) загружаемого файла.
6.8. При возникновении подозрения на наличие вирусов работники обязаны:
6.8.1. приостановить все операции, связанные с обработкой файлов на АРМ;
6.8.2. запустить антивирусное ПО для тестирования файлов, памяти и системных областей дисков;
6.8.3. о факте обнаружения вирусов немедленно сообщить системному администратору, владельцам зараженных или поврежденных вирусами файлов, другим пользователям, использующим зараженные файлы в работе;
6.8.4. провести анализ необходимости дальнейшего использования зараженных вирусом файлов;
6.8.5. провести самостоятельно или совместно с системным администратором лечение зараженных файлов, в случае обнаружения не поддающегося лечению вируса удалить инфицированный файл и проверить работоспособность компьютера.
6.9. Работники допускаются к работе на АРМ только после обучения пользованию средствами антивирусного ПО.

7. Криптографическая защита информации

7.1. Криптографическая защита информации (шифрование) применяется для обеспечения конфиденциальности информации при хранении в ненадежных хранилищах и (или) передаче ее по незащищенным каналам связи (телефон, факс, электронная почта и так далее).
7.2. Применение средств криптографической защиты информации (далее -СКЗИ) для шифрования конфиденциальной информации должно осуществляться с учетом

требований приказа Федеральной службы безопасности Российской Федерации от 09 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

7.3. Необходимость криптографической защиты информации конфиденциального характера при ее обработке в информационной системе, выбор применяемых СКЗИ устанавливаются в зависимости от класса информационной системы в соответствии с правовым актом города Перми, определяющим порядок эксплуатации информационной системы.

7.4. Шифрование осуществляется перед отправкой данных по незащищенным каналам связи или перед помещением на хранение в ненадежных хранилищах.

8. Регламентация использования электронной почты

8.1. Система электронной почты используется в информационных целях, в том числе оповещения, организации работы, обеспечения внутренних и внешних коммуникаций.

8.2. Регламентация использования электронной почты осуществляется с целью снижения риска умышленной или неумышленной несанкционированной рассылки информации, заражения информационных ресурсов ОУ вирусами.

8.3. Угрозы, связанные с электронной почтой:

8.3.1. возможность создания писем с фальшивыми адресами;

8.3.2. возможность нарушения конфиденциальности электронных писем;

8.3.3. возможность изменения в процессе передачи содержимого электронных писем;

8.3.4. осуществление сетевых атак посредством отправки упакованного в архив сообщения, распаковка которого приводит к выводу системы из строя, заражения

8.3.5. получение спама.

8.4. Использование электронной почты в целях исполнения должностных обязанностей работниками осуществляется с использованием индивидуального электронного адреса

8.5. При работе с электронной почтой работники обязаны:

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

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

8.5.3. проверять сообщения электронной почты на наличие вирусов;

8.6. При работе с электронной почтой работникам запрещено:

8.6.1. отправлять сообщения с иного электронного почтового ящика или от имени другого служащего без предоставления полномочий;

8.6.2. 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;

8.6.3. 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;

8.6.4. перехватывать, изменять, удалять, сохранять или публиковать сообщения иных работников, кроме случаев, санкционированных руководителями или в целях администрирования систем;
8.6.5. 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.

9. Регламентация работы в сети Интернет

9.1. Сеть Интернет в ОУ используется работниками для получения информации в рамках исполнения должностных обязанностей.
9.2. Регламентация работы в сети Интернет осуществляется с целью снижения риска заражения информационных ресурсов ОУ вирусами.
9.3. Угрозы, связанные с работой в сети Интернет:
9.3.1. легкость перехвата данных и фальсификации IP-адресов в сети Интернет;
9.3.2. заражение вирусами.
9.4. Работникам запрещается:
9.4.1. осуществлять действия, запрещенные законодательством Российской Федерацией;
9.4.2. отправлять конфиденциальную информацию без предварительного шифрования криптографическим ПО, разрешенным к использованию в ОУ;
9.4.3. 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;
9.4.4. самостоятельно устанавливать на АРМ дополнительное ПО, полученное в сети Интернет;
9.4.5. загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным ПО;
9.4.6. открывать страницы сайтов, если имеются сомнения в надежности сайта и (или) имеются уведомления 0 возможном заражении вирусами.
9.5. Работники обязаны при обнаружении попыток несанкционированного доступа и (или) при подозрении на наличие вируса немедленно прекратить работу в сети Интернет и сообщить системному администратору.
9.6. Вся информация о ресурсах, посещаемых работниками, автоматически протоколируется и при необходимости представляется системными администраторами руководителям.
9.7. Доступ к сети Интернет может быть блокирован системным администратором без предварительного уведомления служащего при возникновении угрозы безопасности информации.

10. Проведение внутреннего контроля и обучение работников

10.1. В целях выявления угроз безопасности информации, нарушений настоящей Политики ИБ и принятия мер, направленных на предотвращение угроз и нарушений, в ОУ осуществляется внутренний контроль:
10.1.1. использования технических средств, ПО, работы в сети Интернет
10.1.2. обработки персональных данных
10.1.3. 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.

10.2. Ознакомление работников с настоящей Политикой ИБ производится при:

10.2.1. приеме на работу;

10.2.2. изменении настоящей Политики ИБ;

10.2.3. обнаружении действий работников, которые повлекли или могли повлечь нарушение безопасности информации.

10.3. Обучение работников пользованию средствами антивирусного ПО производится при:

10.4. приеме на работу;

10.5. изменении антивирусного ПО;

10.6. заражении АРМ вирусами.

10.7. Ознакомление работников 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

10.7.1. фамилии, имени, отчества служащего

10.7.2. даты ознакомления (прохождения обучения).

10.7.3. Обязанность по организации ознакомления работников с настоящей Политикой ИБ возлагается на директора ОУ.

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

11. Ответственность за нарушения настоящей Политики ИБ

11.1. Работники в рамках должностных обязанностей и полномочий несут ответственность в соответствии с действующим законодательством Российской Федерации за:

11.1.1. невыполнение требований настоящей Политики ИБ;

11.1.2. действия или бездействие, ведущие к нарушению информационной безопасности;

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

11.2. При обнаружении нарушения работниками настоящей Политики ИБ системный администратор устанавливает причины возникновения нарушения и направляет служебную записку о выявленном нарушении руководителю ОУ.

11.3. Руководитель ОУ принимает решение о необходимости привлечения служащего к ответственности.

11.4. Системный администратор ведет учет всех выявленных случаев нарушения безопасности информации.