Утверждено

Приказ № СЭД-059-01-10-274

от 30.10.2017

ПОЛИТИКА

информационной безопасности МАОУ «СОШ №50» г. Перми

Общие положения

Настоящая Политика информационной безопасности МАОУ «СОШ№50» г. (далее - Политика ИБ) разработана в целях установления безопас­ных способов обработки информации.

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;

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.

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;

ПО – программное обеспечение.

ПК – персональный компьютер.

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».

Цели и задачи защиты информации, основные виды угроз безопасности информации

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

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.

Угрозы безопасности информации могут быть реализованы за счет:

-утечки по техническим каналам утечки информации;

-несанкционированного доступа с использованием соответствующего про­граммного обеспечения.

-проявление в виде инциден­тов информационной безопасности: утрата информации, оборудования или устройств; системные сбои или перегрузки;

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

компьютере;

-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.

В качестве методов защиты информации применяются:

1. разграничение доступа к техническим средствам и информационным ресурсам;

2. применение антивирусной защиты;

3. регламентация использования электронной почты;

4. регламентация работы в сети Интернет;

5. проведение внутреннего контроля и обучение сотрудников;

6. Ответственность за нарушения настоящей Политики ИБ.

1. Разграничение доступа к техническим средствам и информационным ресурсам

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.

К работе с информационными ресурсами допускаются сотрудники, ознакомленные с настоящей Политикой ИБ.

Для осуществления доступа к информационным ресурсам сотруднику

создают учетная запись - присваивается уникаль­ный идентификатор (имя, логин) и пароль доступа.

Для защиты своих паролей сотрудники обязаны:

-соблюдать конфиденциальность пароля - не сообщать пароль другим ли­цам, в том числе другим служащим, не хранить пароли в легкодоступных местах (на столе, стене, терминале и так далее);

-выбирать трудно угадываемый 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 так далее);

-использовать в пароле не менее 8 символов;

-в случае компрометации пароля немедленно изменить пароль.

При работе на компьютере сотрудники обязаны:

-работать только под своей учетной записью.

Сотрудникам запрещается самостоятельно устанавливать на компьютер допол­нительные технические средства и (или) ПО.

1. Применение антивирусной защиты.

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).

Антивирусное ПО должно быть развернуто на всех технических сред­ствах, подверженных воздействию вирусов. Антивирусные ме­ханизмы должны быть актуальными, постоянно включенными. Отключение антивирусного ПО или отказ от автоматического обновления антивирусных баз не допускается.

При установке антивирусного ПО системным администратором должны выполняться следующие требования:

-актуализация антивирусных баз на ПК, подключенных к локальной сети администрации города Перми, должна осуществляться ежедневно в автоматиче­ском режиме;

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

Некоторые признаки проявления вируса:

-прекращение работы или неправильная работа ранее успешно функциони­ровавшего ПО;

-медленная работа;

-невозможность загрузки операционной системы;

-нетипичная работа ПО;

-вывод на экран непредусмотренных сообщений или изображений;

-подача непредусмотренных звуковых сигналов;

-частые зависания и сбои в работе;

-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.

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

-убедиться, что на ПК 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 антивирусного ПО;

-при переносе на свой ПК 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 ПК, запуская антивирусное ПО для тестирования файлов, памяти и системных областей дисков.

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.

При возникновении подозрения на наличие вирусов сотрудники обязаны:

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

-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. Регламентация использования электронной почты.

Система электронной почты (далее - электронная почта) используется в информационных целях, в том числе оповеще­ния, организации работы, обеспечения внутренних и внешних коммуникаций.

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

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.

При работе с электронной почтой сотрудники обязаны:

-периодически удалять из электронного почтового ящика ненужные сообще­ния и перемещать необходимые сообщения в архивные почтовые папки; проверять сообщения электронной почты на наличие вирусов.

При работе с электронной почтой сотрудникам запрещено:

-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 служащих, кроме случаев, санкционированных руководителями или в целях администрирования систем;

-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. Регламентация работы в сети Интернет.

Сеть Интернет используется сотрудниками для получения информации в рамках исполнения должностных обязанно­стей.

Регламентация работы в сети Интернет осуществляется с целью сни­жения риска заражения информационных ресурсов вирусами.

Угрозы, связанные с работой в сети Интернет:

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

-заражение вирусами.

Сотрудникам запрещается:

-осуществлять действия, запрещенные законодательством Российской Феде­рации;

-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 ПК 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.

Служащие обязаны при обнаружении попыток несанкционированного доступа и (или) при подозрении на наличие вируса немедленно прекратить работу в сети Интернет и сообщить системному администратору.

Доступ к сети Интернет может быть блокирован системным админи­стратором без предварительного уведомления сотрудника при возникновении угрозы безопасности информации.

1. Проведение внутреннего контроля и обучение сотрудников.

В целях выявления угроз безопасности информации, нарушений настоящей Политики ИБ и принятия мер, направленных на предотвращение угроз и нарушений осуществляется внутренний контроль:

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.

Обучение сотрудников пользованию средствами антивирусного ПО производится при:

-приеме на работу;

-изменении антивирусного ПО;

-заражении ПК вирусами.

Ознакомление служащих 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 обучению пользованию средствами антивирусного ПО возлагается на системных администраторов.

1. Ответственность за нарушения настоящей Политики ИБ.

Служащие 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.

При обнаружении нарушения служащими настоящей Политики ИБ системный администратор устанавливает причины возникновения нарушения и направляет служебную записку о выявленном нарушении руководителю функционального (территориального) органа (подразделения) администрации

города Перми.

Системный администратор ведет учет всех выявленных случаев нарушения безопасности информации.