Муниципальное автономное общеобразовательное учреждение
средняя общеобразовательная школа № 3 Малышевского городского округа

МАОУ СОШ № 3

Подписано цифровой подписью: Директор Т.И. Базанова
2021.02.08 16:56:16+05'00'

УТВЕРЖДЕНО:
приказом от 12.03.2014г. № 36/од
Директор МАОУ СОШ № 3
_____ Т.И.Базанова

ПОЛОЖЕНИЕ
об организации системы информационной безопасности в учреждении

ПОЛОЖЕНИЕ
об организации системы информационной безопасности в учреждении

1. Общие положения

1.1. Положение об организации системы информационной безопасности в учреждении (далее Положение) устанавливает систему информационной безопасности в Муниципальном автономном общеобразовательном учреждении средней общеобразовательной школе № 3 (далее – учреждение).

1.2. Настоящее Положение разработано в соответствии с Трудовым кодексом РФ, Федеральным законом от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных", Федеральным законом от 29.12.2010г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию.

1.3. Информационная безопасность (ИБ) является одним из составных элементов комплексной безопасности учреждения. Под информационной безопасностью учреждения понимается состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.

1.4. Система информационной безопасности (СИБ) учреждения включает комплекс правовых, организационных и технических мер, направленных на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.

1.5. Основные понятия, используемые в Положении:

информация - сведения (сообщения, данные) независимо от формы их представления;

информационные технологии (ИТ) - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

информационная система (ИС) - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

доступ к информации - возможность получения информации и ее использования;

конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

1.7. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
2) своевременное обнаружение фактов несанкционированного доступа к информации;
3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
6) постоянный контроль за обеспечением уровня защищенности информации.

2. Доступ к информации

2.1. Информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.
2.2. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).
2.3. Информация в зависимости от порядка ее предоставления или распространения подразделяется на:
1) информацию, свободно распространяемую;
2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя.
2.4. Условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение устанавливаются федеральным законодательством.
2.5. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.
2.6. В учреждении используются следующие формы информации:
- хранение информации на компьютерах;
- передача информации по локальным сетям и через Интернет;
- хранение информации на бумажных носителях;
- сканирование документации;
- передача информации через факс;
- озвучивание (указания, распоряжения, информационные совещания).
2.7. В целях реализации полномочий государственных органов и обеспечения обмена информацией между учреждением и этими органами, а также в иных установленных федеральными законами целях, в учреждении применяются государственные (региональные, муниципальные) информационные системы, при эксплуатации которых учреждение предоставляет статистическую и иную документированную информацию.

Особенности эксплуатации в учреждении государственных (региональных) информационных систем и муниципальных информационных систем устанавливаются в соответствии с техническими регламентами, нормативными правовыми актами государственных органов, нормативными правовыми актами органов местного самоуправления, принимающих решения о создании таких информационных систем.

Порядок создания и эксплуатации информационных систем, не являющихся государственными информационными системами или муниципальными информационными системами, определяется операторами таких информационных систем в соответствии с требованиями, установленными действующим законодательством РФ.

Требования о защите информации, содержащейся в государственных и муниципальных информационных системах, устанавливаются нормативно-правовыми актами соответствующего уровня в пределах их полномочий.

2.8. При использовании сети Интернет в учреждении обучающимся предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и которые имеют прямое отношения к образовательному процессу. Проверка выполнения такого требования осуществляется с помощью программного обеспечения контентной фильтрации, установленного в учреждении.

Запрещенной для распространения среди детей, относится информация:

- побуждающая детей к совершенствованию действий, предоставляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
- способная вызвать у детей желание употребить наркотические вещества, психотропные и одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством и попрошайничеством;
- обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным;
- содержащая информацию порнографического характера;
- оправдывающая противоправное поведение.

Допуск к информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети Интернет, в местах доступных для детей предоставляется лицом, организующим доступ к сети Интернет в таких местах (за исключением операторов связи, оказывающих эти услуги связи на основании договоров об оказании услуг связи, заключенных в письменной форме), другим лицам при условии применения административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации. Причиняющих вред их здоровью и (или) развитию.

Условия и порядок использования сети Интернет в учреждении регулируются Правилами использования сети Интернет (приложение 1).

3.Система информационной безопасности

3.1. СИБ учреждения должна быть направлена на обеспечение:

- конфиденциальности (защиты информации от несанкционированного раскрытия или перехвата);
- целостности (точности и полноты информации и компьютерных программ);
- доступности (возможности получения пользователями информации в пределах их компетенции).

Защита информации регулируется федеральным законодательством и иными нормативными актами и представляет собой принятие правовых, организационных и технических мер.

3.2. Безопасная эксплуатация ИС учреждения включает следующие компоненты:

- информационная безопасность: обеспечение сохранности, целостности и работоспособности информационных ресурсов, профилактика несанкционированного доступа, использования, копирования или удаления информации, а также изменения структуры информационных ресурсов;
- технологическая безопасность: обеспечение стабильности функционирования технических компонентов ИС, предупреждение нецелесообразного использования, нарушения работоспособности, преждевременного износа, повреждения или уничтожения оборудования;
- техническая безопасность: предупреждение или минимизация неблагоприятного воздействия оборудования на организм пользователя, нарушения правил техники безопасности при использовании оборудования, профилактика поражения пользователей электрическим током, тепловым или световым излучением;
- организационная безопасность: предупреждение использования оборудования лицами, не владеющими необходимыми пользовательскими компетентностями, профилактика использования оборудования в целях, не соответствующих целям деятельности учреждения.

3.3. Организация СИБ в учреждении требует проведения следующих первоочередных мероприятий:

1) защита компьютеров, локальных сетей и сети подключения к системе Интернета в классе информатики;
2) организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся;
3) учет всех носителей конфиденциальной информации;
4) защита интеллектуальной собственности учреждения.

3.4. Обеспечение СИБ в учреждении осуществляется по следующим направлениям:

1) правовая защита – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
2) организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;
3) инженерно-техническая защита – это использование различных технических средств, препятствующих нанесению ущерба.

3.5. Безопасная эксплуатация компонентов ИС обеспечивается организационными, программными и аппаратными средствами, человеческими ресурсами.

3.5.1. Организационными средствами обеспечения безопасности ИС учреждения являются:

- разработка нормативных документов, регламентирующих вопросы безопасной эксплуатации ИС;
- проведение инструктажей работников и учащихся по безопасному использованию компонентов ИС учреждения;
- упорядочивание форм использования компонентов ИС учреждения;
- регламентация учетной и контрольной деятельности;

3.5.2. Программными средствами обеспечения безопасности ИС являются:

- организация антивирусного мониторинга и защиты;
- обеспечение контроля входящего и исходящего трафика;
- администрирование доступа к информационным ресурсам Интернет;
- применение автоматизированных систем программного менеджмента.

3.5.3. Аппаратными средствами обеспечения безопасности ИС являются:

- применение аппаратных средств маршрутизации;
- применение устройств бесперебойного питания;
- применение параллельных файловых серверов;
- применение резервного копирования и создание копий информационных ресурсов;

- применение средств охранной сигнализации и видеонаблюдения в местах размещения технических компонентов ИС учреждения.

3.5.4. Ограничение физического доступа к объектам ИС и реализация режимных мер осуществляется при выполнении следующих мероприятий:

- организация и поддержание надежного пропускного режима, контроль посетителей;
- назначение ответственных лиц, контроль работы персонала;
- заключение договоров о материальной ответственности;
- порядок учета, хранения и уничтожения документов;
- установка соответствующих паролей на ЭВМ;
- служба охраны.

3.6. Организационно-технические меры защиты включают следующие основные мероприятия:

1) резервирование (наличие всех основных компонентов операционной системы и программного обеспечения в архивах, копирование таблиц распределения файлов дисков, ежедневное ведение архивов изменяемых файлов);

2) профилактика (систематическая выгрузка содержимого активной части винчестера на дискеты, раздельное хранение компонентов программного обеспечения и программ пользователей, хранение неиспользуемых программ в архивах);

3) ревизия (обследование вновь получаемых программ на дискетах и дисках на наличие вирусов, систематическая проверка длин файлов, хранящихся на винчестере, использование и постоянная проверка контрольных сумм при хранении и передаче программного обеспечения, проверка содержимого загрузочных секторов винчестера и используемых дискет системных файлов);

4) фильтрация (разделение винчестера на логические диски с различными возможностями доступа к ним, использование резидентных программных средств слежения за файловой системой);

Все эти мероприятия, в той или иной степени, включают использование различных программных средств защиты. К их числу необходимо отнести программу-архиватор, программы резервирования важных компонентов файловой системы, просмотра содержимого файлов и загрузочных секторов, подсчета контрольных сумм, контент-фильтры и собственно программы защиты.

3.7. Перечень защищаемых информационных ресурсов и баз данных определяется приложением 2 настоящего Положения.

3.9. Обработка электронных ресурсов, содержащих персональные данные работников и учащихся, проводится строго в соответствии с нормами законодательства Российской Федерации на основании личного согласия работников и родителей учащихся.

4. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации

3.1. Нарушение требований законодательства РФ в области защиты информации влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

3.2. Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

3.3. В случае если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации не несет лицо, оказывающее услуги:
1) либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;
2) либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.
3.4. Трудовой кодекс РФ определяет защиту персональных данных работника. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами".

Положение рассмотрено на педагогическом совете
(протокол № 8 от 24.02.2014г.)

Правила
использования сети Интернет

1. Общие положения

1.1. Использование сети Интернет в учреждении направлено на решение задач учебно-воспитательного процесса.
1.2. Настоящие Правила регулируют условия и порядок использования сети Интернет в Муниципальном автономном общеобразовательном учреждении средней общеобразовательной школе № 3.
1.3. Настоящие Правила имеют статус локального нормативного акта учреждения.

2. Организация использования сети Интернет в образовательном учреждении

2.1. Во время уроков и других занятий в рамках учебного плана, при осуществлении внеурочной деятельности контроль использования обучающимися сети Интернет осуществляет педагогический работник, ведущий занятие (мероприятие); во время свободного доступа к сети Интернет вне учебных занятий – педагогический работник учреждения, за которым закреплен компьютер, с которого осуществляется выход в Интернет.

При этом педагогический работник:

- наблюдает за использованием компьютера и сети Интернет обучающимися;
- принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу;
- ставит в известность классного руководителя о преднамеренных попытках обучающегося осуществить обращение к ресурсам, не имеющим отношения к образовательному процессу.

2.2. При использовании сети Интернет в учреждении обучающимся предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и которые имеют прямое отношения к образовательному процессу. Проверка выполнения такого требования осуществляется с помощью программного обеспечения контентной фильтрации, установленного в школе
2.3. Отнесение определенных ресурсов и (или) категорий ресурсов в соответствующие группы, доступ к которым регулируется программным обеспечением контентной фильтрации обеспечивается должностным лицом по информационным технологиям (в соответствии с должностной инструкцией или назначенным приказом руководителя учреждения).
2.4. Принципы размещения информации на интернет-ресурсах школы призваны обеспечивать:

- соблюдение действующего законодательства Российской Федерации, интересов и прав граждан;
- защиту персональных данных обучающихся, учителей и сотрудников;
- достоверность и корректность информации.

3. Использование сети Интернет в образовательном учреждении

3.1. Использование сети Интернет в школе осуществляется, как правило, в целях образовательного процесса.
3.2. Сотрудники и обучающиеся вправе:

- размещать собственную информацию в сети Интернет на интернет-ресурсах школы;
- иметь учетные записи на интернет-ресурсах школы.

3.3. Сотрудникам и обучающимся запрещается:
- обращаться к ресурсам, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают законодательство Российской Федерации (эротика, порнография, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности);
- осуществлять любые сделки через Интернет;
- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

3.4. Обучающимся не разрешается осуществлять загрузки файлов на школьные компьютер без специального разрешения преподавателя.

3.5. 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 ответственному должностному лицу.

Должностное лицо, ответственное за использование в образовательном процессе информационных технологий, обязано:
- принять информацию от учителя;
- направить информацию о некатегоризированном ресурсе разработчику программы «Интернет Цензор» (в течение суток);
- в случае явного нарушения обнаруженным ресурсом законодательства Российской Федерации сообщить о нем по специальной «горячей линии» (http://skf.edu.ru) для принятия мер в соответствии с законодательством Российской Федерации (в течение суток).

Передаваемая информация должна содержать:
- доменный адрес ресурса;
- сообщение о тематике ресурса, предположения о нарушении ресурсом законодательства Российской Федерации либо его несовместимости с задачами образовательного процесса;
- дату и время обнаружения.

Перечень защищаемых информационных ресурсов и баз данных

№№ пп	объект	Мероприятия	Информационные ресурсы и базы данных
1	система делопроизводства	- учет всей документации учреждения, в т. ч. и на электронных носителях; - регистрация документов, с которых делаются копии, в специальном журнале; - особый режим уничтожения документов; - обработка электронных ресурсов, содержащих персональные данные	Входящая и исходящая документация, Документы учреждения, Портал Е-услуги
2	бухгалтерия	- обработка электронных ресурсов, содержащих персональные данные	Средства ПО 1С: «Заработная плата и кадры»
3	кабинет информатики	- выделенная локальная сеть - контентная фильтрация	сеть Интернет
4	библиотека	- выявления литературы и материалов, содержащих информацию экстремистской направленности	Библиотечный фонд
5	ответственные должностные лица	- ограниченный доступ при обработке информации, содержащей персональные данные обучающихся и работников учреждения в региональной информационной системе	РИС (ГИА), «КАИС», КПМО, файловый сервер РЦОИ и др.