Утверждено приказом директора
от 10.06.2024 № 156

Положение об информационной безопасности

1. Общие положения

1.1. Информационная безопасность является одним из составных элементов комплексной безопасности в Муниципальном автономном общеобразовательном учреждении «Городская гимназия № 1» (далее — Гимназия), порядок организации работ по её созданию и функционированию.

1.2. Данное положение разработано в соответствии с Федеральным законом Российской Федерации от 29 декабря 2012 г. № 273-ФЗ "Об образовании в Российской Федерации", Трудовым кодексом РФ от 30.12.2001 № 197-ФЗ (с изм. и доп.), Федеральным законом от 29.12.2012 г. №273-ФЗ «Об образовании в Российской Федерации», 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" и имеет статус локального нормативного акта образовательной организации. Если нормами действующего законодательства РФ предусмотрены иные требования, чем настоящим Положением, применяются нормы законодательства РФ.

1.3. Под информационной безопасностью Гимназия следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности. Система информационной безопасности направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию.

1.4. Использование сети Интернет в образовательной организации подчинено следующим принципам:

- соответствие образовательным целям;

- способствование гармоничному формированию и развитию личности;

- уважение закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей сети Интернет;

- приобретение новых навыков и знаний;

- расширение применяемого спектра учебных и наглядных пособий;

- социализация личности, введение в информационное общество.

1.5. К объектам информационной безопасности в Гимназии относятся:

- информационные ресурсы, содержащие конфиденциальную информацию, представленную в виде документированных информационных массивов и баз данных;

- информацию, защита которой предусмотрена законодательными актами РФ, в т. ч. персональные данные;

- средства и системы информатизации — средства вычислительной и организационной техники, локальной сети, общесистемное и прикладное программное обеспечение, автоматизированные системы управления рабочими местами, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации.

1.6. Система информационной безопасности (далее - СПБ) должна обязательно обеспечивать:

- конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);

- целостность (точность и полноту информации и компьютерных программ);

- доступность (возможность получения пользователями информации в пределах их компетенции).

1.7. Обеспечение информационной безопасности осуществляется по следующим направлениям:

- правовая зашита – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

- организационная зашита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;

- инженерно-техническая защита – это использование различных технических средств, препятствующих нанесению ущерба.

2. Цели и задачи обеспечения безопасности информации

2.1. Главной целью обеспечения безопасности информации, циркулирующей в Гимназии, является реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации ограниченного доступа (далее по тексту - конфиденциальной или защищаемой информации) и предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационной среды Гимназии.

2.2. Основными целями обеспечения безопасности информации являются:

- предотвращение утечки, хищения, искажения, подделки информации, циркулирующей в Гимназии;

- предотвращение нарушений прав личности обучающихся, работников Гимназии на сохранение конфиденциальности информации;

- предотвращение несанкционированных действий по блокированию информации.

2.3. Основными задачами обеспечения безопасности информации являются:

- соответствие положениям законодательных актов и нормативным требованиям по защите информации;

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба интересам Гимназии, нарушению нормального функционирования и развития Гимназии;

- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции в системе информационных отношений;

- эффективное пресечение незаконных посягательств на информационные ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;

- развитие системы защиты, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий ее нарушения;

- развитие и совершенствование защищенного юридически значимого электронного документооборота;

- создание механизмов, обеспечивающих контроль системы информационной безопасности и гарантии достоверности выполнения установленных требований информационной безопасности;

- создание механизмов управления системой информационной безопасности.

3. Правовые нормы обеспечения информационной безопасности

3.1. Гимназия имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников Гимназии, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.

3.2. Гимназия обязана обеспечить сохранность конфиденциальной информации.

3.3. Администрация Гимназии:

- назначает ответственного за обеспечение информационной безопасности;

- издаёт нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;

- имеет право включать требования по обеспечению информационной безопасности в коллективный договор;

- имеет право включать требования по защите информации в договоры по всем видам деятельности;

- разрабатывает перечень сведений конфиденциального характера;

- имеет право требовать защиты интересов Гимназии со стороны государственных и судебных инстанций.

3.4. Организационные и функциональные документы по обеспечению информационной безопасности:

- приказ директора Гимназии о назначении ответственного за обеспечение информационной безопасности;

- должностные обязанности ответственного за обеспечение информационной безопасности;

- перечень защищаемых информационных ресурсов и баз данных;

- инструкция, определяющая порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников Гимназии и др.

3.5. Порядок допуска сотрудников Гимназии к информации предусматривает:

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;

- ознакомление работника с нормами законодательства РФ и Гимназии об информационной безопасности и ответственности за разглашение информации конфиденциального характера;

- инструктаж работника специалистом по информационной безопасности;

- контроль работника ответственным за информационную безопасность при работе с информацией конфиденциального характера.

4. Использование сети Интернет

4.1. Использование сети Интернет в Гимназии осуществляется в целях образовательного процесса. В рамках развития личности, ее социализации и получения знаний в области компьютерной грамотности лицо может осуществлять доступ к ресурсам не образовательной направленности.

4.2. Работники Гимназии вправе:

- размещать информацию в сети Интернет на интернет-ресурсах Гимназии;

- иметь учетную запись электронной почты на интернет-ресурсах Гимназии.

4.3. Работникам Гимназии запрещено размещать в сети Интернет и на образовательных ресурсах информацию:

- противоречащую требованиям законодательства РФ и локальным нормативным актам Гимназии;

- не относящуюся к образовательному процессу и не связанную с деятельностью Гимназии;

- нарушающую нравственные и этические нормы, требования профессиональной этики.

4.4. Обучающиеся Гимназии вправе:

- использовать ресурсы, размещенные в сети Интернет, в том числе интернет-ресурсы Гимназии, в порядке и на условиях, которые предусмотрены настоящим Положением.

- размещать информацию и сведения на интернет-ресурсах Гимназии.

4.5. Обучающемся запрещено:

- находиться на ресурсах, содержание и тематика которых недопустима для несовершеннолетних и/или нарушает законодательство РФ;

- в осуществлять любые сделки через интернет;

- загружать файлы на компьютер Гимназии без разрешения уполномоченного лица;

- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

4.6. Запрет и снятие такого запрета на допуск пользователей к работе в сети Интернет устанавливает уполномоченное лицо, назначенное приказом директора Гимназии.

4.7. Если в процессе работы пользователем будет обнаружен ресурс, содержимое которого не совместимо с целями образовательного процесса, он обязан незамедлительно сообщить об этом уполномоченному лицу с указанием интернет-адреса (URL) и покинуть данный ресурс.

4.8. Уполномоченное лицо обязано:

- принять сообщение пользователя;

- принять меры по отключению выхода на данный ресурс с интернет ресурсов Гимназии;

- если обнаруженный ресурс явно нарушает законодательство РФ - сообщить о нем по специальной «горячей линии» для принятия мер в соответствии с законодательством РФ (в течение суток).

Передаваемая информация должна содержать:

- интернет-адрес (URL) ресурса;

- тематику ресурса, предположения о нарушении ресурсом законодательства РФ либо несовместимости с задачами образовательного процесса;

- дату и время обнаружения;

- информацию об установленных в образовательной организации технических средствах ограничения доступа к информации.

5. Мероприятия по обеспечению информационной безопасности

5.1. Для обеспечения информационной безопасности в Гимназии требуется проведение следующих первоочередных мероприятий:

- защита интеллектуальной собственности Гимназии;

- защита компьютеров, локальных сетей и сети подключения к системе Интернета;

- организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся Гимназии;

- учет всех носителей конфиденциальной информации.

6. Организация работы с информационными ресурсами и технологиями

6.1. Система организации делопроизводства:

- учет всей документации Гимназии, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;

- регистрация и учет всех входящих (исходящих) документов Гимназии в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);

- регистрация документов, с которых делаются копии, в специальном журнале (дата копирования, количество копий, для кого или с какой целью производится копирование);

- особый режим уничтожения документов.

6.2. В ходе использования, передачи, копирования и исполнения документов также необходимо соблюдать определенные правила:

6.2.1. Документы, дела и издания с грифом «Для служебного пользования» («Ограниченного пользования») должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах. При этом должны быть созданы условия, обеспечивающие их физическую сохранность.

6.2.2. Выданные для работы дела и документы с грифом «Для служебного пользования» («Ограниченного пользования») подлежат возврату в канцелярию в тот же день.

6.2.3. Передача документов исполнителю производится только через ответственного за организацию делопроизводства.

6.2.4. Запрещается выносить документы с грифом «Для служебного пользования» за пределы Гимназии.

6.2.5. При смене работников, ответственных за учет и хранение документов, дел и изданий, составляется по произвольной форме акт приема передачи документов.

6.3. Для организации делопроизводства приказом директора Гимназии назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации

делопроизводства, утвержденной директором Гимназии. Контроль за порядком его ведения возлагается на ответственного за информационную безопасность.

7. О системном администрировании и обязанностях ответственного за информационную безопасность.

7.1. Задачи, связанные с мерами системного администрирования, обеспечивающего информационную безопасность, являются частью работы ответственного за информатизацию в МАОУ «Городская гимназия № 1».

7.2. Для решения задач информационной безопасности ответственный за информатизацию обязан:

- следить за соблюдением требований по парольной защите, в том числе осуществлять изменение паролей по мере необходимости (утрата пароля, появление новых пользователей в связи с изменением кадрового состава и пр.);

- обеспечивать функционирование программно-аппаратного комплекса защиты по внешним цифровым линиям связи;

- обеспечивать мероприятия по антивирусной защите, как на уровне серверов, так и на уровне пользователей;

- обеспечивать нормальное функционирование системы резервного копирования.

8. Антивирусная защита Правила пользования внешними сетевыми ресурсами (Интернет, электронная почта и т.д.):

8.1. Основным способом проникновения компьютерных вирусов на компьютер пользователя в настоящее время является Интернет и электронная почта. В связи с этим на компьютерах, используемых учащимися в учебной деятельности, устанавливается программное обеспечение, блокирующее доступ к негативной информации, которое обеспечено провайдером и программной поддержкой браузера (фильтр-контент);

8.2. Обучающимся закрыт доступ к сети Интернет через Wi-fi в местах общего пользования Гимназии (библиотеки, коридоры и учебные кабинеты) с помощью пароля и прокси-сервера;

8.3. Исключена возможности установки на школьные компьютеры игр и другого ПО не связанных с образовательным процессом. Обучающиеся работают за компьютерами исключительно в присутствии и под руководством педагогов;

8.4. Мониторинг качества работы системы контентной фильтрации в ОО проводится ежедневно.