ОБЩЕОБРАЗОВАТЕЛЬНОЕ АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ «ЦЕНТР ОБРАЗОВАНИЯ «ЛИЧНОСТЬ»
(ОАНО «Центр образования «Личность»)

ПРИНЯТО
на педагогическом совете
(протокол № 1 от «30» августа 2023г.)

УТВЕРЖДАЮ
Директор _____/ Л.А. Израилова/
Прик. №118 от 01.09.2023г.

СОГЛАСОВАНО
С Советом Центра образования

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 01DA5A900071AF278746E407F7C1945487
Владелец: ОАНО "ЦЕНТР ОБРАЗОВАНИЯ "ЛИЧНОСТЬ"
Действителен: с 20.12.2022 до 20.03.2024

Положение об информационной безопасности.

1. Общие положении

1.1. Информационная безопасность является одним из составных элементов комплексной безопасности

1.2. Данное положение разработано в соответствии с Трудовым кодексом РФ от 30.12.2001 № 197-ФЗ (с изм. и доп.). 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".

1.3. Под информационной безопасностью школы 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. К объектам информационной безопасности в школе относятся: • информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера: • информацию, защита которой предусмотрена законодательными актами РФ. в т. ч. персональные данные: • средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

1.5. Система информационной безопасности (далее - СИБ) 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). 1.6 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. Правовые нормы обеспечения информационной безопасности

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

2.2. Школа обязана обеспечить сохранность конфиденциальной информации.

2.3. Администрация школы: • 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 школы со стороны государственных и судебных инстанций.

2.4. Организационные и функциональные документы по обеспечению информационной безопасности: • приказ директора школы 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 школы и др.

2.5. порядок допуска сотрудников школы к информации предусматривает: • принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера; • ознакомление работника с нормами законодательства РФ и школы 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.

3. Мероприятия по обеспечению информационной безопасности Для обеспечения информационной безопасности в школе требуется проведение следующих первоочередных мероприятий: • защита интеллектуальной собственности школы; • защита компьютеров, локальных сетей и сети подключения к системе Интернета; • организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся школы; • учет всех носителей конфиденциальной информации.

4. Организация работы с информационными ресурсами и технологиями

4.1. Система организации делопроизводства: • учет всей документации школы, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию; • регистрация и учет всех входящих (исходящих) документов школы 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.

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

4.2.1. Все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов.

4.2.2. 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.

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

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

4.2.5. Запрещается выносить документы с грифом "Для служебного пользования" за пределы школы.

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

4.3.Для организации делопроизводства приказом директора школы назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной директором школы. Контроль за порядком его ведения возлагается на ответственного за информационную безопасность.

5. Обеспечение безопасности в Школьном портале

5.1. Школьный портал относится к группе многопользовательских информационных систем с разными правами доступа. С учетом особенностей обрабатываемой информации, система соответствует требованиям, предъявляемым действующим в Российской Федерации законодательством, к информационным системам, осуществляющим обработку персональных данных. Школьный портал обеспечивает возможность защиты информации от потери и несанкционированного доступа на этапах её передачи и хранения. Для настройки прав пользователей в системе созданы отдельные роли пользователей с назначением разрешений на выполнение отдельных функций и ограничений по доступу к информации, обрабатываемой в Школьном портале.

5.2. Регламент общих ограничений для участников образовательного процесса при работе со «Школьным порталом, обеспечивающей предоставление Услуги.

5.2.1.Участники образовательного процесса, имеющие доступ к Школьному порталу, не имеют права передавать персональные логины и пароли для входа на Школьный портал другим лицам. Передача персонального логина и пароля для входа в Школьный портал другим лицам влечет за собой ответственность в соответствии с законодательством Российской Федерации о защите персональных данных.

5.2.2.Участники образовательного процесса, имеющие доступ к Школьному порталу, соблюдают конфиденциальность условий доступа в свой личный кабинет (логин и пароль).

5.2.3.Участники образовательного процесса, имеющие доступ к Школьному порталу, в случае нарушения конфиденциальности условий доступа в личный кабинет, уведомляют в течение не более чем одного рабочего дня со дня получения информации о таком нарушении руководителя ОО, службу технической поддержки Школьного портала.

5.2.4.Все операции, произведенные участниками образовательного процесса, имеющими доступ к Школьному порталу, с момента получения информации руководителем ОО и службой технической поддержки о нарушении, указанном в предыдущем абзаце, признаются недействительными.

5.2.5.При проведении работ по обеспечению безопасности информации в Школьном портале участники образовательного процесса, имеющие доступ к Школьному порталу,

обязаны соблюдать требования законодательства Российской Федерации в области защиты персональных данных

ПЕДАГОГАМ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Когда речь заходит об информационной безопасности, обычно мы начинаем думать о компьютерах, сетях, интернете и хакерах. Но для образовательной среды проблема стоит шире: в ограждении учащегося от информации, которая может негативно повлиять на его формирование и развитие, то есть о пропаганде различной направленности.

Понятие информационной безопасности

Под информационной безопасностью понимается защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации.

На практике важнейшими являются три аспекта информационной безопасности:

- доступность (возможность за разумное время получить требуемую информационную услугу);
- целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- конфиденциальность (защита от несанкционированного прочтения).

Нарушения доступности, целостности и конфиденциальности информации могут быть вызваны различными опасными воздействиями на информационные компьютерные системы.

Основные угрозы информационной безопасности

Современная информационная система представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя. Компоненты автоматизированной информационной системы можно разбить на следующие группы:

- ***Аппаратные средства.*** Это компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства – принтеры, контроллеры, кабели, линии связи и т.д.);
- ***Программное обеспечение.*** Это приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т.д.;
- ***Данные,*** хранимые временно и постоянно, на дисках, флэшках, печатные, архивы, системные журналы и т.д.;

- ***Персонал.*** Пользователи, системные администраторы, программисты и др.
- Опасные воздействия на компьютерную информационную систему можно подразделить на случайные и преднамеренные. Анализ опыта проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни системы. Причинами случайных воздействий при эксплуатации могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания;
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе персонала;
- помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные воздействия – это целенаправленные действия нарушителя. В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами:

- недовольством служащего своей карьерой;
- взяткой;
- любопытством;
- конкурентной борьбой;
- стремлением самоутвердиться любой ценой.

Можно составить гипотетическую модель потенциального нарушителя:

- квалификация нарушителя на уровне разработчика данной системы;
- нарушителем может быть как постороннее лицо, так и законный пользователь системы;
- нарушителю известна информация о принципах работы системы;
- нарушитель выбирает наиболее слабое звено в защите.

Наиболее распространенным и многообразным видом компьютерных нарушений является несанкционированный доступ. Несанкционированный доступ использует любую ошибку в системе защиты и возможен при нерациональном выборе средств защиты, их некорректной установке и настройке.

Проведем классификацию каналов несанкционированного доступа, по которым можно осуществить хищение, изменение или уничтожение информации:

Через человека:

- хищение носителей информации;
- чтение информации с экрана или клавиатуры;
- чтение информации из распечатки.

Через программу:

- перехват паролей;
- дешифровка зашифрованной информации;
- копирование информации с носителя.

Через аппаратуру:

- подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации;
- перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и т.д.

Особо следует остановиться на угрозах, которым могут подвергаться компьютерные сети. Основная особенность любой компьютерной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Компьютерные сети характерны тем, что против них предпринимают так называемые удаленные атаки. Нарушитель может находиться за тысячи километров от атакуемого объекта, при этом нападению может подвергаться не только конкретный компьютер, но и информация, передающаяся по сетевым каналам связи.

Обеспечение информационной безопасности

Формирование режима информационной безопасности – проблема комплексная. Меры по ее решению можно подразделить на пять уровней:

1. Законодательный . Это законы, нормативные акты, стандарты и т.п.

Нормативно-правовая база определяющая порядок защиты информации:

2. Морально-этический. Всевозможные нормы поведения, несоблюдение которых ведет к падению престижа конкретного человека или целой организации.

3. Административный. Действия общего характера, предпринимаемые руководством организации. Такими документами могут быть:

- приказ руководителя о назначении ответственного за обеспечение информационной безопасности;
- должностные обязанности ответственного за обеспечение информационной безопасности;
- перечень защищаемых информационных ресурсов и баз данных;
- инструкцию, определяющую порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников организации.

4. Физический. Механические, электро- и электронно-механические препятствия на возможных путях проникновения потенциальных нарушителей.

5. Аппаратно-программный (электронные устройства и специальные программы защиты информации).

Принятые меры по созданию безопасной информационной системы в школе:

- Обеспечена защита компьютеров от внешних несанкционированных воздействий (компьютерные вирусы, атаки хакеров и т. д.)
- Установлен строгий контроль за электронной почтой, обеспечен постоянный контроль за входящей и исходящей корреспонденцией.
- Установлены соответствующие пароли на персональные ПК.
- Использованы контент-фильтры, для фильтрации сайтов по их содержимому.

Единая совокупность всех этих мер, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба, образуют систему защиты.

Специалисты, имеющие отношение к системе защиты должны полностью представлять себе принципы ее функционирования и в случае возникновения затруднительных ситуаций адекватно на них реагировать. Под защитой должна находиться вся система обработки информации.

Лица, занимающиеся обеспечением информационной безопасности, должны нести личную ответственность.

Надежная система защиты должна быть полностью протестирована и согласована. Защита становится более эффективной и гибкой, если она допускает изменение своих параметров со стороны администратора.

В заключение своего доклада хотелось бы дать некоторые рекомендации по организации работы в информационном пространстве, чтобы уберечь себя и своих близких от интернет-преступников.

Рекомендации по организации работы в информационном пространстве

1. Перед началом работы необходимо четко сформулировать цель и вопрос поиска информации.

2. Желательно выработать оптимальный алгоритм поиска информации в сети Интернет, что значительно сократит время и силы, затраченные на поиск.

3. Заранее установить временный лимит (2-3 часа) работы в информационном пространстве (просмотр телепередачи, чтение, Интернет).

4. Во время работы необходимо делать перерыв на 5-10 минут для снятия физического напряжения и зрительной нагрузки.

5. Необходимо знать 3-4 упражнения для снятия зрительного напряжения и физической усталости.

6. Работать в хорошо проветренном помещении, при оптимальном освещении и в удобной позе.

7. Не стоит легкомысленно обращаться со спам-письмами и заходить на небезопасные веб-сайты. Для интернет-преступников вы становитесь лёгкой добычей.

8. При регистрации в социальных сетях, не указывайте свои персональные данные, например: адрес или день рождения.

9. Не используйте в логине или пароле персональные данные.

10. Все это позволяет интернет-преступникам получить данные доступа к аккаунтам электронной почты, а также инфицировать домашние ПК для включения их в бот-сеть или для похищения банковских данных родителей.

11. Создайте собственный профиль на компьютере, чтобы обезопасить информацию, хранящуюся на нем.

12. Не забывайте, что факты, о которых вы узнаете в Интернете, нужно очень хорошо проверить, если выбудете использовать их в своей домашней работе. Целесообразно сравнить три источника информации, прежде чем решить, каким источникам можно доверять.

13. О достоверности информации, помещенной на сайте можно судить по самому сайту, узнав об авторах сайта.

14. Размещая информацию о себе, своих близких и знакомых на страницах социальных сетей, спросите предварительно разрешение у тех, о ком будет эта информация.

15. Не следует размещать на страницах веб-сайтов свои фотографии и фотографии своих близких и знакомых, за которые вам потом может быть стыдно.

16. Соблюдайте правила этики при общении в Интернете: грубость провоцирует других на такое же поведение.

17. Используя в своей работе материал, взятый из информационного источника (книга, периодическая печать, Интернет), следует указать этот источник информации или сделать на него ссылку, если материал был вами переработан.