ПЕДАГОГАМ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Проблема обеспечения информационной безопасности школьников является актуальной особенно в условиях информатизации образования, когда каждый учащийся имеет личные электронные устройства и открытый доступ в Интернет.

Информационная безопасность - это не только обеспечение безопасности персональных данных и знакомство с ососновными правилами безопасного использования сети Интернет.

Для образовательной среды проблема стоит шире: в ограждении учащегося от информации, которая может негативно повлиять на его формирование и развитие.

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, логические бомбы, 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.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

по обеспечению информационной безопасности в образовательной организации основного общего образования

1. Общие положения

1.1. Методические рекомендации по обеспечению информационной безопасности (далее-методические рекомендации) разработаны в соответствии с ФЗ-152 от 27.07.2006г. «О персональных данных», ФЗ149 от 27.07.2006г. «Об информации, информационных технологиях и о защите информации», ФЗ-273 от 29.12.2012г. «Об образовании в Российской Федерации».

1.2. Методические рекомендации предназначены для руководящих и педагогических работников образовательных организаций основного общего образования.

1.3. Методические рекомендации определяют необходимый перечень требований по обеспечению безопасности информации в образовательных организациях основного общего образования.

1.4. Методические рекомендации разработаны для использования образовательными организациями основного общего образования при работе с персональными данными учащихся, их родителей или законных представителей, педагогического состава и иных работников образовательной организации с целью защиты персональных данных и недопущения утечки информации, содержащей сведения персональных данных.

2. Основные понятия

2.1. Информация — сведения (сообщения, данные) независимо от формы их представления;

2.2. Информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

2.3. Информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

2.4. Информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

2.5. 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;

2.6. Доступ к информации — возможность получения информации и ее использования;

2.7. Конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

2.8. Предоставление информации — действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

2.9. Распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

2.10. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.11. Информационная система персональных данных — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

3. Персональные данные: понятие, сущность, обработка.

3.1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) согласно ФЗ-152 «О персональных данных» от 27.07.2006г. Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайны. Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. Образовательные учреждения попадают под это понятие и являются операторами персональных данных. Под обработкой персональных данных понимается любое действие или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных. При обработке персональных данных оператор обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.2. К персональным данным в образовательной организации основного общего образования относятся:

- Фамилия имя отчество (далее по тексту — Ф.И.О.) сотрудников организации;
- Ф.И.О. учащихся;
- Ф.И.О. родителей или законных представителей учащихся;
- Сведения, содержащиеся в основном документе, удостоверяющем личность субъекта;
- Информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования;
- Сведения, содержащиеся в документах воинского учета для военнообязанных и лиц, подлежащих призыву на военную службу;
- Сведения об образовании, квалификации или наличии специальных знаний или подготовки;
- Сведения, содержащиеся в свидетельстве о постановке на учёт физического лица в налоговом органе на территории Российской Федерации;
- Сведения о семейном положении;
- Биометрические персональные данные — сведения, которые характеризуют физиологические и биологические особенност и человека, наоснованиии которых можно установить его личность (биометричес

кие персональные данные) и которые используются оператором для установления личности субъекта персональных данных;
- Информация медицинского характера, в случаях, предусмотренных Законодательством;
- Сведения о заработной плате работников, родителей учащихся;
- Сведения о социальных льготах;
- Сведения о наличии судимостей.

Памятка педагогам по обеспечению информационной безопасности обучающихся (воспитанников)

- Объясните учащимся правила поведения в Интернете. Расскажите о мерах, принимаемых к нарушителям, ответственности за нарушение правил поведения в сети.
- Совместно с учащимися сформулируйте правила поведения в случае нарушения их прав в Интернете.
- Приучайте несовершеннолетних уважать права других людей в Интернете. Объясните им смысл понятия «авторское право», расскажите об ответственности за нарушение авторских прав.
- Проявляйте интерес к «виртуальной» жизни своих учеников, и при необходимости сообщайте родителям о проблемах их детей.
- Научите учеников внимательно относиться к информации, получаемой из Интернета. Формируйте представление о достоверной и недостоверной информации. Настаивайте на посещении проверенных сайтов.
- Обеспечьте профилактику интернет-зависимости учащихся через вовлечение детей в различные внеклассные мероприятия в реальной жизни (посещение театров, музеев, участие в играх, соревнованиях), чтобы показать, что реальная жизнь намного интереснее виртуальной.
- Периодически совместно с учащимися анализируйте их занятость и организацию досуга, целесообразность и необходимость использования ими ресурсов сети для учебы и отдыха с целью профилактики интернет-зависимости и обсуждайте с родителями результаты своих наблюдений.
- В случае возникновения проблем, связанных с Интернет-зависимостью, своевременно доводите информацию до сведения родителей, привлекайте к работе с учащимися и их родителями психолога, социального педагога.
- Проводите мероприятия, на которых рассказывайте о явлении Интернет-зависимости, ее признаках, способах преодоления.
- Систематически повышайте свою квалификацию в области информационно-коммуникационных технологий, а также по вопросам здоровьесбережения.
- Станьте примером для своих учеников. Соблюдайте законодательство в области защиты персональных данных и информационной безопасности. Рационально относитесь к своему здоровью. Разумно используйте в своей жизни возможности интернета и мобильных сетей.
- Перед началом работы необходимо четко сформулировать цель и вопрос поиска информации.
- Желательно выработать оптимальный алгоритм поиска информации в сети Интернет, что значительно сократит время и силы, затраченные на поиск.
- Заранее установить временный лимит (2-3 часа) работы в информационном пространстве (просмотр телепередачи, чтение, Интернет).
- Во время работы необходимо делать перерыв на 5-10 минут для снятия физического напряжения и зрительной нагрузки.

- Не стоит легкомысленно обращаться со спам-письмами и заходить на небезопасные веб-сайты. Для интернет-преступников вы становитесь лёгкой добычей.
- При регистрации в социальных сетях, не указывайте свои персональные данные, например: адрес или день рождения.
- Не используйте в логине или пароле персональные данные.
- 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.
- Создайте собственный профиль на компьютере, чтобы обезопасить информацию, хранящуюся на нем.
- 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.
- О достоверности информации, помещенной на сайте можно судить по самому сайту, узнав об авторах сайта.
- Размещая информацию о себе, своих близких и знакомых на страницах социальных сетей, спросите предварительно разрешение у тех, о ком будет эта информация.
- Не следует размещать на страницах веб-сайтов свои фотографии и фотографии своих близких и знакомых, за которые вам потом может быть стыдно.
- Соблюдайте правила этики при общении в Интернете: грубость провоцирует других на такое же поведение.
- 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.

Списки информационных материалов и сайтов, содержащих информацию, распространение которой в Российской Федерации запрещено

- Федеральный список экстремистских материалов
- Единый реестр сайтов в сети «Интернет», содержащих запрещенную информацию

РЕКОМЕНДУЕМ

- Единый урок по безопасности в сети «Интернет»
- https://stepik.org/Безопасность-в-интернете-191/ «Безопасность в интернете»- курс от Академии Яндекса.

Курс для школьников 6—9 классов, но он будет полезен и родителям, а также учителям, планирующим рассказывать в школе о безопасном использовании интернета, например, во время Всероссийского урока по безопасности в интернете, или проводить уроки финансовой грамотности. В курсе три раздела. Каждый раздел состоит из конспекта для самостоятельного изучения, видео-урока и теста, помогающего лучше усвоить изученный материал. Мы надеемся, что курс поможет юным пользователям интернета не попасться на удочку мошенников.

- http://www.ligainternet.ru/encyclopedia-of-security/parents-and-teachers/parents-and-teachers-detail.php?ID=3652 -Лига безопасного Интернета: уроки безопасного Интернета. Здесь вы найдёте разнообразные материалы к урокам безопасного Интернета.

- http://www.saferunet.ru/ -На сайте «Центр безопасного интернета в России» полезная информация для детей, подростков и взрослых.
- https://мвд.рф/document/1910260 -Интернет-мошенничество. Памятка МВД для граждан.
- Линия помощи «Дети онлайн» — бесплатная всероссийская служба телефонного и онлайн консультирования для детей и взрослых по проблемам безопасного использования интернета и мобильной связи.
- Горячая Линия Фонда Дружественный Рунет.
- Федеральная программа безопасного детского интернета Гогуль.
- Интернет и дети. Советы по безопасности от лаборатории Касперского.
- Правила безопасной работы в интернете от компании Microsoft.
- Ролики по безопасному использованию интернета от компании Google .
- Рекомендации парламентских слушаний «Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве».
- Методические рекомендации по проведению Единого урока по безопасности в сети «Интернет».
- Методические рекомендации для проведения лекций и бесед в образовательных учреждениях и на «Родительских уроках» по теме предупреждение и методы защиты от преступных посягательств в отношении несовершеннолетних.
- Методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.
- Рекомендации корпорации Google «Детская безопасность».
- Тест Лаборатории Касперского «Киберграмотен ли ты?».
- Методические рекомендации по основам информационной безопасности для обучающихся общеобразовательных организаций с учётом информационных, потребительских, технических и коммуникативных аспектов информационной безопасности
- Урок цифры «Безопасность в интернете»
- Видеоурок «Безопасность в Интернете»
- МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ по организации и проведению в школах Российской Федерации тематических уроков «Безопасность в Интернете» в рамках Всероссийской образовательной акции «Урок цифры»
- Рекомендации Минпросвещения России «Безопасность в интернете»
- Классный час «За стеной отчуждения»: правила безопасного поведения в виртуальном пространстве.
- Классный час на тему «Безопасность в Интернете касается всех, касается каждого!»
- Видео-уроки информационной безопасности
- **Брошюры и лифлеты** (ссылки для скачивания):

- Скачать брошюру
- Вредоносные программы в интернете
- Владельцам пластиковых банковских карт
- Пользователям интернета
- Телефонные мошенники
- Безопасный интернет — детям