

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.

ПЕДАГОГАМ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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.

ПЕДАГОГАМ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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.

ПЕДАГОГАМ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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.

ПЕДАГОГАМ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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.

ПЕДАГОГАМ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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.)

ПЕДАГОГАМ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

Под защитой должна находиться вся система обработки информации.

Некоторые рекомендации по организации работы в информационном пространстве, чтобы уберечь себя и своих близких от интернет-преступников.

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.

ПЕДАГОГАМ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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. Систематически повышайте свою квалификацию в области информационно-коммуникационных технологий, а также по вопросам здоровьесбережения.
12. Исключить применение иностранных систем видеоконференции связи, в том числе Zoom, Skype, а также систем удаленного доступа (RAdmin, TeamViewer);
13. **Необходимо регулярно создавать резервные копии всех важных документов на внешних носителях.**
14. Ответственность за обеспечение защиты информации на рабочем месте пользователя возлагается непосредственно на пользователя (потребителя информации).