С. Н. Анкуда

ФУНКЦИОНАЛЬНАЯ ГРАМОТНОСТЬ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: МИФ ИЛИ РЕАЛЬНОСТЬ?

10–11 классы

ДИДАКТИЧЕСКИЕ МАТЕРИАЛЫ

Пособие для учащихся учреждений образования, реализующих образовательные программы общего среднего образования, с белорусским и русским языками обучения и воспитания

С. Н. Анкуда

ФУНКЦИОНАЛЬНАЯ ГРАМОТНОСТЬ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: МИФ ИЛИ РЕАЛЬНОСТЬ?

10–11 классы

ДИДАКТИЧЕСКИЕ МАТЕРИАЛЫ

Пособие для учащихся учреждений образования, реализующих образовательные программы общего среднего образования, с белорусским и русским языками обучения и воспитания

Рекомендовано
научно-методическим учреждением
«Национальный институт образования»
Министерства образования
Республики Беларусь

Учебное электронное издание

Минск
Национальный институт образования
2023

УДК 004.056(075.3)
ББК 32.81я721

Р е ц е н з е н т ы:

кафедра защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (доктор технических наук, профессор, заведующий кафедрой *Т. В. Борботько*);

учитель информатики квалификационной категории «учитель-методист» государственного учреждения образования «Средняя школа № 4 г. Дзержинска» *С. Г. Пузиновская*

Данное пособие входит в учебно-методический комплекс по формированию функциональной грамотности «Информационная безопасность: миф или реальность?», 10–11 классы.

Учебно-методический комплекс факультативных занятий разработан в Национальном институте образования в рамках выполнения задания ОНТП «Функциональная грамотность» и включен в сводный план выпуска (внедрения) вновь освоенной продукции (инноваций) по ОНТП «Функциональная грамотность» на 2021–2025 гг., утвержденный Министерством образования от 17.02.2021. Язык издания — русский.

Нач. редакционно-издательского отдела *С. П. Малявко*
Редактор *Л. Ф. Левкина*
Компьютерная вёрстка *Я. И. Архиповой*

Подписано к использованию 2023
Размещено на сайте 2023

Объем издания 952 КБ
Системные требования: ПО для просмотра документов в формате pdf

Научно-методическое учреждение «Национальный институт образования»
Министерства образования Республики Беларусь.
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий № 1/263 от 02.04.2014.
Ул. Короля, 16, 220004, г. Минск

ISBN 978-985-893-570-2

ОГЛАВЛЕНИЕ

10 класс

11 класс

10 класс

ГЛАВА 1
СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

10 класс (35 часов)

Тема 1. Главные понятия в области пользования и защиты информации. Основные причины обострения проблемы обеспечения информационной безопасности (10 часов)

Материал для ознакомления

Компонент, связанный с компьютерной грамотностью и безопасностью учащихся, выходит на одно из первых мест. Навык взаимодействия с электронными сервисами требуется уже по окончании учреждения общего среднего образования.

Компьютерная грамотность, как одна из составляющих функциональной грамотности, заключается в умениях:

- работать с информацией в Интернете, искать и анализировать данные, сегментировать их по степени достоверности;
- пользоваться электронными сервисами: почтой, облачными хранилищами, базовыми программами;
- знать правила безопасности и защиты личной информации, управлять личными аккаунтами в соцсетях.

Важно знать о различных проявлениях киберугроз: Интернет-зависимость, мошеннические действия в Интернете, вторжение в персональные данные, насилие в Интернете, навязчивая реклама — и способах борьбы с ними. Наиболее эффективным в данном случае будет решение ситуационных и проблемных задач, выполнение индивидуальных и групповых проектов в сфере информационной безопасности и принятие соответствующих решений.

Программа факультативных занятий включает изучение теоретических основ информационной безопасности в контексте нормативно-правовых требований, законодательной базы (девиз: «Внимание: персональные данные!»), выполнение заданий, отражающих реальные ситуации, заданий по решению проблем информационной и кибербезопасности с использованием специальных аппаратно-программных средств (девиз: «Интернет известный и неизвестный»).

Информационная безопасность — это практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная или, например, физическая); это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, с целью нанесения ущерба владельцам или пользователям информации.

Основная задача информационной безопасности — сбалансированная защита конфиденциальности, целостности и доступности данных с учетом целесообразности

применения и без какого-либо ущерба производительности организации. Это достигается, в основном, посредством многоэтапного процесса управления рисками, который позволяет идентифицировать основные средства и нематериальные активы, источники угроз, уязвимости, потенциальную степень воздействия и возможности управления рисками.

Угрозы информационной безопасности могут быть классифицированы по различным признакам:

- ✓ по аспекту информационной безопасности, на который направлены угрозы:
  - угрозы конфиденциальности (неправомерный доступ к информации). Угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Она имеет место, когда получен доступ к некоторой информации ограниченного доступа, хранящейся в информационной системе или передаваемой от одной системы к другой. В связи с угрозой нарушения конфиденциальности используется термин «утечка». Подобные угрозы могут возникать вследствие «человеческого фактора» (например, случайное делегирование тому или иному пользователю привилегий другого пользователя), сбоев в работе программных и аппаратных средств. К информации ограниченного доступа относится государственная тайна и конфиденциальная информация (коммерческая тайна, персональные данные, профессиональные виды тайн: врачебная, адвокатская, банковская, служебная, нотариальная, тайна страхования, следствия и судопроизводства, переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений (тайна связи), сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации (ноу-хау) и др.);
  - угрозы целостности (неправомерное изменение данных). Угрозы нарушения целостности — это угрозы, связанные с вероятностью модификации той или иной информации, хранящейся в информационной системе. Нарушение целостности может быть вызвано различными факторами — от умышленных действий персонала до выхода из строя оборудования;
  - угрозы доступности (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы). Нарушение доступности представляет собой создание таких условий, при которых доступ к услуге или информации будет либо заблокирован, либо возможен за время, которое не обеспечит выполнение тех или иных бизнес-целей;
- ✓ по расположению источника угроз:
  - внутренние (источники угроз располагаются внутри системы);
  - внешние (источники угроз находятся вне системы);
- ✓ по размерам наносимого ущерба:
  - общие (нанесение ущерба объекту безопасности в целом, причинение значительного ущерба);
  - локальные (причинение вреда отдельным частям объекта безопасности);
  - частные (причинение вреда отдельным свойствам элементов объекта безопасности);
- ✓ по степени воздействия на информационную систему:
  - пассивные (структура и содержание системы не изменяются);
  - активные (структура и содержание системы подвергается изменениям);

✓ по природе возникновения:
- естественные (объективные) — вызванные воздействием на информационную среду объективных физических процессов или стихийных природных явлений, не зависящих от воли человека;
- искусственные (субъективные) — вызванные воздействием на информационную сферу человека. Среди искусственных угроз в свою очередь выделяют:
  - непреднамеренные (случайные) угрозы — ошибки программного обеспечения, персонала, сбои в работе систем, отказы вычислительной и коммуникационной техники;
  - преднамеренные (умышленные) угрозы — неправомерный доступ к информации, разработка специального программного обеспечения, используемого для осуществления неправомерного доступа, разработка и распространение вирусных программ и т. д. Преднамеренные угрозы обусловлены действиями людей. Основные проблемы информационной безопасности связаны прежде всего с умышленными угрозами, так как они являются главной причиной преступлений и правонарушений.

Все источники угроз информационной безопасности можно разделить на три основные группы:

1. Обусловленные действиями субъекта (антропогенные источники) — субъекты, действия которых могут привести к нарушению безопасности информации. Данные действия могут быть квалифицированы как умышленные или случайные преступления. Источники, действия которых могут привести к нарушению безопасности информации, бывают как внешними, так и внутренними. Эти источники можно спрогнозировать, и принять адекватные меры.
2. Обусловленные техническими средствами (техногенные источники) — эти источники угроз менее прогнозируемы, напрямую зависят от свойств техники и поэтому требуют особого внимания. Данные источники угроз информационной безопасности также могут быть как внутренними, так и внешними.
3. Стихийные источники — данная группа объединяет обстоятельства, составляющие непреодолимую силу (стихийные бедствия или другие обстоятельства, которые невозможно предусмотреть или предотвратить или возможно предусмотреть, но невозможно предотвратить), такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. Эти источники угроз совершенно не поддаются прогнозированию, поэтому меры против них должны применяться всегда. Стихийные источники являются внешними по отношению к защищаемому объекту и под ними, как правило, понимаются природные катаклизмы.

Задачи информационной безопасности сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий.

Таким образом, информационная безопасность — многогранная область деятельности, в которой успех может принести только систематический, комплексный подход.

Обеспечение информационной безопасности в большинстве случаев связано с комплексным решением задач:
- обеспечение доступности информации;
- обеспечение целостности информации;

- обеспечение конфиденциальности информации;
- обеспечение достоверности информации.

Именно доступность, целостность и конфиденциальность являются равнозначными составляющими информационной безопасности. Информационные системы создаются для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, то это наносит ущерб всем пользователям.

Доступность — это гарантия получения требуемой информации или информационной услуги пользователем за определенное время. Фактор времени в определении доступности информации в ряде случаев является очень важным, поскольку некоторые виды информации и информационных услуг имеют смысл только в определенный промежуток времени. Например, получение заранее заказанного билета на самолет после его вылета теряет всякий смысл. Точно так же получение прогноза погоды на вчерашний день не имеет никакого смысла, поскольку это событие уже наступило.

Целостность информации условно подразделяется на статическую и динамическую. Статическая целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации. Динамическая целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др.

Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например техническими, социальными и т. д.

Ошибка в управляющей программе приведет к остановке управляемой системы, неправильная трактовка закона может привести к его нарушениям, точно также неточный перевод инструкции по применению лекарственного препарата может нанести вред здоровью. Все эти примеры иллюстрируют нарушение целостности информации, что может привести к катастрофическим последствиям. Именно поэтому целостность информации выделяется в качестве одной из базовых составляющих информационной безопасности.

Целостность — гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.

Конфиденциальность информации — характеристика, которая указывает на необходимость ограничить доступ к информационным ресурсам для определенного круга лиц. В процессе действий и операций информация становится доступной только пользователям, которые успешно прошли идентификацию.

Достоверность указывает на принадлежность информации доверенному лицу или владельцу, который одновременно выступает в роли источника информации.

Классификация Интернет-угроз:

1. Контентные риски.

Контентные риски связаны с потреблением информации, которая публикуется в Интернете и включает в себя незаконный и неподобающий контент. В зависимости

от культуры, законодательства, менталитета и узаконенного возраста согласия в стране определяется группа материалов, считающихся неподобающими. Неподобающий контент включает в себя материалы, содержащие насилие, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр и наркотических веществ.

2. Незаконный контент.

В зависимости от законодательства страны разные материалы могут считаться нелегальными. В большинстве стран запрещены материалы сексуального характера с участием детей и подростков, порнографический контент, описания насилия, в том числе сексуального, экстремизм и разжигание расовой ненависти.

3. Электронная безопасность.

Риски, связанные с электронной безопасностью, относятся к различной кибердеятельности, которая включает в себя: а) разглашение персональной информации, б) выход в сеть с домашнего компьютера с низким уровнем защиты (риск подвергнуться вирусной атаке), в) онлайн-мошенничество и г) спам.

4. Вредоносные программы.

Вредоносные программы — это программы, негативно воздействующие на работу компьютера. К ним относятся вирусы, программы-шпионы, нежелательное рекламное ПО и различные формы вредоносных кодов.

5. Спам.

Спам — это нежелательные электронные письма, содержащие рекламные материалы. Спам дорого обходится для получателя, так как пользователь тратит на получение большего количества писем свое время и оплаченный Интернет-трафик. Также нежелательная почта может содержать вредоносные программы в виде самозапускающихся вложений.

6. Кибермошенничество.

Кибермошенничество — это один из видов киберпреступления, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким-либо образом использует личную информацию пользователя с целью получения материальной прибыли. Есть несколько видов кибермошенничества: нигерийские письма, фишинг, вишинг и фарминг.

7. Коммуникационные риски.

Коммуникационные риски связаны с межличностными отношениями Интернет-пользователей и включают в себя контакты с возможными преступниками и киберпреследования.

8. Незаконный контакт.

Незаконный контакт — это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения.

9. Киберпреследования.

Киберпреследование — преследование человека сообщениями, содержащими оскорбления, агрессию с помощью Интернет-коммуникаций. Киберпреследование может принимать такие формы, как обмен информацией, контактами или изображениями, запугивание, подражание, хулиганство (Интернет-троллинг) и социальное бойкотирование.

Вредоносные программы

Вредоносные программы — это приложения или код, которые препятствуют нормальному использованию конечных устройств. Когда устройство заражено вредоносной программой, вы можете столкнуться с несанкционированным доступом, компрометацией данных или блокировкой и требованием заплатить выкуп.

Вредоносные программы обманывают пользователей и мешают нормальной работе с устройствами. Как только киберпреступник получает доступ к вашему устройству с помощью одного или нескольких различных методов — например фишингового письма, зараженного файла, уязвимости системы или программного обеспечения, зараженного USB-накопителя или вредоносного веб-сайта — он использует ситуацию в своих интересах, чтобы проводить дополнительные атаки, получить учетные данные, собирать личную информацию для продажи, продавать доступ к вычислительным ресурсам или вымогать оплату у жертв.

Ниже описаны несколько способов, с помощью которых киберпреступники пытаются заразить устройства вредоносными программами.

Фишинг

Во время фишинговой атаки вы получаете электронное письмо, текстовое сообщение, открываете веб-сайт или взаимодействуете с любой другой формой коммуникации, напоминающей ресурс, которому можно доверять. Так работает механизм реализации вредоносной программы. Обычно во время таких атак могут быть украдены имена пользователей, пароли, сведения платежных карт или данные банковских счетов. Атаки такого типа могут привести к хищению персональных данных или краже денег напрямую со счета или банковской карты. Например, киберпреступник может выдать себя за представителя известного банка и отправить клиенту электронное письмо с предупреждением о том, что его счет был заморожен из-за подозрительных действий, и требованием перейти по ссылке в письме, чтобы решить проблему. После нажатия на такую ссылку устанавливается вредоносная программа.

Программа-шпион

Программа-шпион устанавливается на устройстве сама без чьего-либо согласия или предупреждения. После установки она может отслеживать поведение в Сети, собирать конфиденциальные данные, менять параметры устройства и ухудшать его производительность.

Программа для показа рекламы

Программа такого типа, как и программа-шпион, устанавливается на устройство сама, без чьего-либо согласия. Такие программы отображают на экране агрессивную рекламу, часто в виде всплывающих объявлений, чтобы пользователь щелкнул рекламу, что может привести к хищению денежных средств. Программы для показа рекламы часто ухудшают производительность устройства. Более опасные программы для показа рекламы могут устанавливать дополнительное ПО, менять параметры браузера и увеличивать уязвимость устройства к другим вредоносным атакам.

Вирусы

Вирусы разработаны для вмешательства в нормальную работу устройства путем записи, повреждения или удаления его данных. Они часто распространяются на устройствах, обманом заставляя людей открывать вредоносные файлы.

Эксплойты и наборы эксплойтов

Эксплойты используют уязвимости ПО, чтобы обойти систему безопасности устройства и заразить его. Хакеры проводят сканирование для поиска устройств с устаревшими системами, содержащими уязвимости, а затем взламывают их и развертывают вредоносные программы. Путем включения кода оболочки в эксплойт киберпреступники могут загрузить больше вредоносных программ, которые заражают устройства и проникают в организации.

Наборы содержат несколько эксплойтов, которые сканируют устройства на разные типы уязвимостей. Если обнаружена уязвимость, наборы развертывают дополнительные вредоносные программы. Среди программ, которые могут быть заражены, встречаются Adobe Flash Player, Adobe Reader, веб-браузеры, Oracle Java и Sun Java. Angler/Axpergle, Neutrino и Nuclear — некоторые типы распространенных наборов эксплойтов.

Обычно эксплойты и наборы эксплойтов используют вредоносные веб-сайты или почтовые вложения для взлома информационной сети либо устройства, но иногда они также прячутся в рекламе на законных веб-сайтах без ведома владельцев сайта.

Вредоносные программы без использования файлов

В эту категорию входят вредоносные программы, которые не используют файлы (например вложения электронной почты) для проникновения в Сеть. Такие программы могут поступать через вредоносные сетевые пакеты, которые используют уязвимость, а затем устанавливают вредоносные программы. Вредоносные программы, не использующие файлы, особенно сложно обнаружить и удалить, так как большинство антивирусов не поддерживает сканирование встроенного ПО.

Вредоносные макросы

Возможно, вы уже знакомы с макросами, которые позволяют быстро автоматизировать рутинные задачи. Вредоносные программы в макросах используют их функциональность, чтобы заражать вложения и файлы архивов ZIP. Чтобы обманом заставить людей открыть файлы, киберпреступники часто прячут вредоносные программы в файлах, замаскированных под счета, квитанции и юридические документы.

В прошлом вредоносные программы для макросов были более распространены, так как макросы запускались автоматически при открытии документа. Но в последних версиях Microsoft Office макросы отключены по умолчанию, а это значит, что киберпреступникам, заражающим устройства таким образом, приходится убеждать пользователей их включить.

Программы-шантажисты

Программа-шантажист — это вредоносная программа, которая угрожает жертве, уничтожая важные данные либо блокируя доступ к ним до тех пор, пока не будет выплачен выкуп. Программы-шантажисты, управляемые человеком, проникают в организацию через общие ошибки в системе безопасности, ориентируются в ее корпоративной сети и адаптируются к среде и любым слабым местам. Распространенным способом получения доступа к сети организации для распространения программы-шантажиста является кража преступником учетных данных реального сотрудника с целью выдать себя за него и получить доступ к его учетной записи.

Пакеты программ rootkit

С помощью пакета программ rootkit киберпреступники могут скрывать вредоносные программы на устройстве очень продолжительное время (иногда даже годы), чтобы непрерывно иметь доступ к сведениям и ресурсам. Перехватывая и изменяя стандартные процессы операционной системы, rootkit может изменять данные устройства, которым оно сообщает о себе. К примеру, устройство, на котором действует rootkit, может отображать неполный список запущенных программ. Пакет программ rootkit также может предоставлять киберпреступникам права администратора или повышенные привилегии, в результате чего они получают полный контроль над устройством и могут выполнять потенциально опасные действия, например, красть данные, следить за жертвой и устанавливать дополнительные вредоносные программы.

Трояны

Троянские программы рассчитаны на то, что пользователь неосознанно скачает их, поскольку они выглядят как официальные файлы или приложения. После скачивания трояны могут:

- скачивать и устанавливать дополнительные вредоносные программы, например вирусы или червей;
- использовать устройство для клик-фрода;
- записывать нажатия клавиш и веб-сайты, которые вы посещаете;
- отправлять информацию (например, пароли, данные для входа и историю просмотров) о зараженном устройстве злоумышленнику;
- предоставлять киберпреступнику контроль над зараженным устройством.

Нежелательные программы

Когда на устройстве установлено нежелательное ПО, пользователь может столкнуться с изменениями в работе веб-браузера, изменением процесса скачивания и установки, вводящими в заблуждение сообщениями и несанкционированным изменением параметров устройства. Некоторые нежелательные программы поставляются в комплекте с программами, которые люди скачивают.

Черви

Червь распространяется по информационной сети, используя уязвимости в системе безопасности и копируя себя, чаще всего во вложениях электронной почты, текстовых сообщениях, программах совместного использования файлов, сайтах социальных сетей, на сетевых ресурсах и съемных дисках. В зависимости от типа червя, он может красть конфиденциальную информацию, изменять настройки безопасности или лишать доступа к файлам.

Вирусы-майнеры

С ростом популярности криптовалют майнинг стал прибыльным занятием. Вирусы-майнеры используют вычислительные ресурсы устройства для майнинга криптовалют. Заражение этим типом вредоносной программы часто начинается с вложения в электронную почту, которое пытается установить вредоносная программа, или с веб-сайта, который использует уязвимости в веб-браузерах или использует вычислительную мощность компьютера для добавления вредоносной программы на устройства.

Классификация методов защиты информации

Все методы защиты информации по характеру проводимых действий можно разделить на законодательные (правовые), организационные, технические, комплексные.

Для обеспечения защиты объектов информационной безопасности должны быть соответствующие правовые акты, устанавливающие порядок защиты и ответственность за его нарушение. Законы должны давать ответы на следующие вопросы: «Что такое информация?», «Кому она принадлежит?», «Как может с ней поступать собственник?», «Что является посягательством на его права?», «Как он может защищаться?», «Какую ответственность несет нарушитель прав собственника информации?».

Установленные в законах нормы реализуются через комплекс организационных мер, проводимых прежде всего государством, ответственным за выполнение законов, и собственниками информации. К таким мерам относятся также издание подзаконных актов, регулирующих конкретные вопросы по защите информации (положения, инструкции, стандарты и т. д.), и государственное регулирование сферы через систему лицензирования, сертификации, аттестации.

Поскольку в настоящее время основное количество информации генерируется, обрабатывается, передается и хранится с помощью технических средств, то для конкретной ее защиты в информационных объектах необходимы технические устройства. В силу многообразия технических средств нападения приходится использовать обширный арсенал технических средств защиты. Наибольший положительный эффект достигается в том случае, когда все перечисленные способы применяются совместно, т. е. комплексно.

Принципы построения систем информационной безопасности:

- системность;
- комплексность;
- непрерывность защиты;
- разумная достаточность;
- гибкость управления и применения;
- открытость алгоритмов и механизмов защиты;
- простота применения защитных методов и средств.

Кроме того, любые используемые средства и механизмы информационной безопасности не должны нарушать нормальную работу пользователя с автоматизированной информационной системой: резко снижать производительность, повышать сложность работы и т. п. Система защиты информации должна быть ориентирована на тактическое опережение возможных угроз, а также обладать механизмами восстановления нормальной работы информационной системы в случае реализации угроз.

Принципы защиты информации от несанкционированного доступа

Закрытие каналов несанкционированного получения информации должно начинаться с контроля доступа пользователей к ресурсам информационной системы. Эта задача решается на основе ряда принципов.

- *Принцип обоснованности доступа* заключается в обязательном выполнении следующего условия: пользователь должен иметь достаточную форму допуска для получения информации требуемого им уровня конфиденциальности с тем, чтобы выполнить заданные производственные функции. В качестве пользователей могут выступать активные программы и процессы, а также носители информации.
- *Принцип разграничения:* для предупреждения нарушения безопасности информации, которое, к примеру, может произойти при записи секретной

информации на несекретные носители и в несекретные файлы, при передаче ее программам и процессам, не предназначенным для обработки секретной информации, а также при передаче секретной информации по незащищенным каналам и линиям связи, необходимо осуществлять соответствующее разграничение потоков информации и прав доступа к этой информации.

- ✓ *Принцип чистоты ресурсов* заключается в очистке ресурсов, содержащих конфиденциальную информацию, при их удалении или освобождении пользователем до перераспределения этих ресурсов другим пользователям.
- ✓ *Принцип персональной ответственности:* каждый пользователь информационной системы должен нести персональную ответственность за свою деятельность в системе, включая любые операции с секретной информацией и возможные нарушения ее защиты, случайные или умышленные действия, которые приводят или могут привести к несанкционированному доступу или, наоборот делают такую информацию недоступной для законных пользователей.
- ✓ *Принцип целостности средств защиты* подразумевает, что средства защиты информации в информационной системе должны точно выполнять свои функции в соответствии с перечисленными принципами и быть изолированными от пользователей. С целью своего сопровождения средства защиты должны включать специальный защищенный интерфейс для средств контроля, сигнализации и фиксирования.

Методы и средства защиты информации

Методы защиты информации:

- *препятствие* — метод физического преграждения пути злоумышленнику к защищаемой информации;
- *управление доступом* — метод определения и распределения ресурсов системы санкционированным пользователям;
- *шифрование* — метод защиты информации в коммуникационных каналах путем ее криптографического закрытия. Этот метод защиты широко применяется как для обработки, так и для хранения информации. При передаче информации по коммуникационным каналам большой протяженности этот метод является единственно надежным;
- *регламентация* — метод защиты информации, создающий специальные условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму;
- *принуждение* — такой метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности;
- *побуждение* — метод защиты информации, который стимулирует пользователя и персонал системы не нарушать установленных норм (высокая зарплата).

Средства защиты информации

- Технические средства защиты информации: реализуются в виде электрических, электромеханических и электронных устройств. Вся совокупность технических средств защиты делится на аппаратные и физические.

Под аппаратными средствами защиты принято понимать встроенные электронные устройства. Из наиболее известных аппаратных средств можно

назвать схемы контроля информации по четности, схемы защиты полей памяти по ключу и другие.

Физические средства защиты реализуются в виде автономных устройств и систем. Например, замки на дверях помещений с аппаратурой, решетки на окнах, охранная сигнализация, камеры видеонаблюдения. Обеспечивают:

– безопасность помещений, где размещены серверы сети;
– ограничение посторонним лицам физического доступа к серверам, концентраторам, коммутаторам, сетевым кабелям и другому оборудованию;
– защиту от сбоев электросети.

- Программные средства представляют собой программное обеспечение, специально предназначенное для выполнения функций защиты информации.

Стандартные защищенные программные средства

Средства защиты, использующие парольную идентификацию и ограничивающие доступ пользователей согласно назначенным правам — управление доступом и разграничение полномочий (идентификация+аутентификация+авторизация).

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова «аутентификация» иногда используют словосочетание «проверка подлинности».

Регистрация и анализ событий, происходящих в системе, обеспечивает получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля, а также регистрацию действий, признанных потенциально опасными для безопасности системы. Анализ собранной информации позволяет выявить средства и априорную информацию, использованные нарушителем при воздействии на систему, и определить, как далеко зашло нарушение, подсказать метод его расследования и способы исправления ситуации.

Контроль целостности ресурсов системы предназначен для своевременного обнаружения их модификации. Это позволяет обеспечить правильность функционирования системы и целостность обрабатываемой информации.

Криптографическое закрытие информации.

Защита от внешних вторжений: брандмауэры.

Защита от компьютерных вирусов: антивирусные пакеты, антиспамовые фильтры.

Средства резервного копирования и восстановления данных.

- Аппаратно-программные средства защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав системы защиты информации и выполняющих (самостоятельно или в комплексе с другими средствами) такие функции защиты, как: идентификация и аутентификация пользователей, разграничение доступа к ресурсам, регистрация событий, криптографическое закрытие информации, обеспечение отказоустойчивости компонента и системы в целом и т. д.
- Организационные средства защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации специального ПО и аппаратных устройств для обеспечения защиты информации.

Организационные мероприятия охватывают все структурные элементы на всех этапах жизненного цикла защищаемой системы (создание охраняемого периметра, строительство помещений, проектирование системы в целом, монтаж и наладка оборудования, испытания и эксплуатация), а также кадровую политику и подбор персонала.

- Морально-этические средства защиты реализуются в виде норм, которые сложились традиционно или складываются по мере распространения информационных технологий и средств связи в данной стране или обществе. Эти нормы, как правило, не являются обязательными, как законодательные меры, однако несоблюдение их ведет к потере авторитета и престижа организации.
- Законодательные средства защиты определяются законодательными актами страны. В них регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

По своему функциональному назначению методы и средства информационной безопасности можно разделить на следующие разновидности:

- методы и средства предупреждения — предназначены для создания таких условий, при которых возможность появления и реализации дестабилизирующих факторов (угроз) исключается или сводится к минимуму;
- методы и средства обнаружения — предназначены для обнаружения появившихся угроз или возможности их появления и сбора дополнительной информации;
- методы и средства нейтрализации — предназначены для устранения появившихся угроз;
- методы и средства восстановления — предназначены для восстановления нормальной работы защищаемой системы (иногда и самой системы защиты).

Практические, ситуационные задания

Задание 1. Основы защиты ПК

1. Очистка корзины и окончательное удаление файлов.

Щелкните правой кнопкой мыши на значке *Корзина* на рабочем столе.

В контекстном меню выберите команду *Свойства*. Отобразится диалоговое окно *Свойства: Корзина*.

Выберите вкладку *Глобальные*.

Установите флажок *Уничтожать файлы сразу после удаления, не помещая их в корзину*.

Щелкните на кнопке *ОК*.

Предупреждение. Помните, что после установки этого параметра вы не сможете восстанавливать удаленные файлы.

Восстановите прежнее состояние *Корзины*.

2. Проверка того, открывал ли кто-нибудь ваш файл во время вашего отсутствия.

Запустите *Проводник*, выбрав его в меню *Программы* из меню *Пуск*.

Откройте каталог, в котором хранится ваш файл.

Щелкните на имени файла правой кнопкой мыши, и в отобразившемся контекстном меню выберите команду *Свойства*.

Вы увидите диалоговое окно свойств файла. В средней части окна приведены дата и время создания файла, а также время его последнего открытия и редактирования.

Если доступ к файлу последний раз предоставлялся уже после того, как вы отошли от ПК, то это означает, что файл кто-то открывал.

Чтобы узнать, использовал ли кто-нибудь для открытия ваших файлов особое, интересующее вас приложение, просмотрите меню *Файл* этого приложения. В нижней части меню вы найдете нумерованный список файлов; это те файлы, которые открывались из данного приложения в последнее время. Если вы заметите имя файла, с которым давно не работали, либо порядок имен файлов отличается от того порядка, в котором работали с файлами в данном приложении вы, значит, кто-то открывал ваш файл (или файлы). В таком случае, просмотрите окно свойств файлов, чтобы получить дополнительную информацию.

Предупреждение. Обязательно проверьте свойства подозрительного файла перед тем, как откроете его. Если вы этого не сделаете, то дата и время последнего открытия файла будут заменены. При открытии файла операционная система Windows немедленно обновляет эту информацию.

Еще один способ контроля несанкционированного доступа к файлам: просмотр меню *Документы* из меню *Пуск*.

3. Удаление своих «следов» из меню *Документы*.

Выполните команду *Пуск > Настройка > Панель задач* и меню *Пуск*. Отобразится диалоговое окно *Свойства: Панель задач*.

В диалоговом окне *Свойства: Панель задач* выберите *Настройка меню* и щелкните на кнопке *Очистить* в области *Меню Документы*.

Задание 2. Простые установки и настройки системы защиты

1. Удаление и переименование пунктов меню *Пуск*.

Удалите из меню *Пуск* игру *Косынка*. Очистите *Корзину*.

Запустите игру *Косынка* (файл Sol.exe)

Восстановите ярлык *Косынка* в меню *Пуск* на прежнем месте.

Переименуйте в меню *Пуск* игру *Косынка* на *SOL*.

2. Скрытие Панели задач.

Щелкните на кнопке *Пуск*.

Щелчком мыши выберите *Настройка > Панель задач* и откройте диалоговое окно *Свойства: Панель задач*.

Щелкнете на вкладке *Параметры панели задач*, если это необходимо.

Щелкните на флажке с надписью *Автоматически убирать с экрана* и на кнопке *ОК*.

Восстановите Панель задач.

3. Зашита от изменения файлов.

Запустите *Проводник*.

Откройте соответствующую папку и правым щелчком мыши выберите предохраняемый вами файл. Далее выберите пункт *Свойства* в отобразившемся контекстном меню.

Щелкните на флажке, отмеченном *Только чтение*, и на кнопке *ОК*. Теперь файл защищен от редактирующих его содержимое изменений.

Задание 3. Система защиты паролем Windows

1. Защита паролем заставки экрана.

Щелкните на пункте *Настройка* меню *Пуск* и выберите пункт *Панель управления*. Выполните двойной щелчок мышью на инструменте *Экран*. (Альтернатива — щелкнуть правой кнопкой мыши на свободной поверхности рабочего стола и выбрать пункт *Свойства*. Отобразится диалоговое окно *Свойства: Экран*.

Щелкните на вкладке *Заставка* (Screen Saver) и на флажке *Пароль* (Pasword Protected). Далее щелкните на кнопке *Изменить* (Change) и в отобразившемся диалоговом окне введите пароль. (Вы должны будете ввести пароль дважды для его подтверждения.)

Предупреждение. Система защиты паролем заставки экрана прекрасно подходит в том случае, если нужно покинуть компьютер на непродолжительное время. Но вы должны учесть основной недостаток этой системы: если кто-то очень захочет войти в ваш компьютер, то все, что ему следует для этого сделать, это перезагрузить компьютер.

2. Создать загрузочный пароль с помощью заставки экрана.

С помощью папки *Проводник* найдите файл .SCR, соответствующий заставке экрана, которую вы хотите активизировать. (Файлы .SCR хранятся в папке windowssystem, их названия соответствуют пунктам списка заставок на странице *Заставка* (Screen Saver) диалогового окна *Свойства: Экран*.

Щелкните правой кнопкой мыши на файле заставки экрана и перетащите его в такую папку Windows/Главное Меню/Программы/Автозагрузка.

После этого появится контекстное меню. Выберите пункт *Создать ярлык*. Теперь установленная заставка экрана будет запускаться вместе с Windows и запрашивать при этом пароль. (Вы должны, конечно, установить для своего рабочего стола пароль, воспользовавшись вкладкой *Заставка* (Screen Saver) диалогового окна *Свойства: Экран*.

3. Сетевая защита паролем для файлов и папок.

Откройте какой-либо файл своего диска для других пользователей Сети (*Проводник* > *открыть Диск С:* > щелкнуть правой кнопкой по файлу > *Свойства* > *Доступ* > кнопка *Общий ресурс*).

Установите тип доступа *«Определяется паролем»*.

Введите пароль для чтения.

Попросите учащегося, работающего на другом компьютере, прочитать ваш файл.

4. Использование бесплатных и условно бесплатных программ для защиты паролем.

Установите на свой компьютер программу Black Magic или Screen Lock.

Защитите с помощью этой программы доступ к вашему компьютеру и проверьте защиту.

Снимите защиту.

5. Защита паролем входа в Windows через систему CMOS.

Выключите компьютер.

Включите компьютер и нажимайте на клавишу Delete (или F1: в зависимости от фирмы, установившей программу ROM BIOS - CMOS Setup), пока не появится окно настройки CMOS.

Раскройте окно установки пароля (Password Setting) и установите пароль.

В строке Security Option окна Bios Features Setup введите System (вместо Setup).

Откройте окно Save & Exit Setup и нажмите Y и Enter.

Запишите введенный пароль.

Проверьте, что установленный пароль работает.

Снимите пароль и перезагрузите компьютер.

Задание 4. Защита файлов и папок

1. Изменение списков последних открывавшихся файлов меню Файл.

Выберите в меню команду *Сервис>Параметры*, а затем выберите вкладку *Общие*.

Установите число нуль в окне *«помнить список из ... файлов»* и нажмите *ОК*.

Откройте меню *Файл* и просмотрите список последних открывавшихся файлов.

Восстановите состояние окна *«помнить список из ... файлов»* по умолчанию.

2. Запутывание «следов» ложными именами файлов и расширениями.

Измените имя своего файла и его расширение.

Откройте приложение *Проводник* и раскройте каталог с файлом, который вы хотите переименовать.

Щелкните на имени файла правой кнопкой мыши.

В отобразившемся контекстном меню выберите команду *Переименовать*.

Введите новое имя файла (как имя, так и расширение).

Нажмите клавишу *Enter*.

Отобразится сообщение: *После смены расширения имени файла этот файл может оказаться недоступным. Вы действительно хотите изменить расширение?* Щелкните на кнопке *Да*.

Запомните прежнее имя и расширение файла.

Попытайтесь открыть этот файл.

Восстановите прежнее имя и расширение файла.

3. Запутывание следов подменой папок.

Задайте папку, которую при открытии файлов приложение просматривает в первую очередь:

а) В приложении Word выполните команду *Сервис>Параметры>Расположение*.

б) В приложении Excel для этого используйте команду *Сервис>Параметры>Общие*.

в) В приложении PowerPoint используйте команду *Сервис>Параметры>Дополнительно*.

Измените имя своей папки.

4. Создание файлов с доступом «только для чтения» и защита паролями.

Сохраните файл при помощи приложения, установив атрибут *«только для чтения»*.

При открытом файле выберите в меню приложения команду *Файл: Сохранить как*. Отобразится диалоговое окно *Сохранение документа*.

В текстовом поле ввода *Имя файла* введите имя файла и зайдите в этом же окне в меню *Сервис>Параметры*. Отобразится диалоговое окно *Сохранение*. (Если данный файл уже сохранялся и, возможно, вновь открывался, просто используйте имя файла в текстовом поле *Имя файла* или щелкните на имени уже существующего файла).

Установите флажок *Рекомендовать доступ только для чтения* в нижнем левом углу диалогового окна *Сохранение*. Щелкните на кнопке *ОК*, а затем, в диалоговом окне *Сохранение документа*, на кнопке *Сохранить*.

Защитите сохраняемый файл паролем.

Выберите в меню приложения команду *Файл>Сохранить как* и зайдите в меню *Сервис>Параметры* в отобразившемся диалоговом окне *Сохранение документа*.

В диалоговом окне *Сохранение* введите пароль в поле *«пароль для открытия файла»*. При желании введите пароль и в поле *«пароль разрешения записи»*,

расположенное рядом. Это позволит вам установить различные уровни доступа к файлу: только для просмотра или с правом редактирования.

После ввода пароля отобразится окно с предложением ввести его повторно для подтверждения.

Примечание. Пароль может состоять из букв и цифр. Буквы, входящие в пароль, чувствительны к регистру; иными словами, если при вводе пароля вы используете прописную букву (или буквы), вы должны использовать прописные буквы и при вводе пароля для открытия документа.

Задание 5. Скрытые файлы, папки и приложения

1. Установка атрибутов файлов и папок.

Познакомьтесь с атрибутами файлов.

Установите для вашего файла атрибут *Скрытый* (Hidden): выполните правый щелчок на имени файла, атрибуты которого вы хотите установить.

В появившемся контекстном меню выберите *Свойства*. На экране появится одноименное диалоговое окно.

Установите для вашего файла атрибут *Скрытый*.

Атрибуты расположены в нижней части диалогового окна. Для установки соответствующего атрибута достаточно установить флажок, щелкнув на нем. Повторный щелчок приведет к отмене атрибута.

Установите для вашей папки атрибут *Скрытый*.

2. Скрытые файлы и папки.

Сделайте невидимым ваш файл.

Установив для файла или папки атрибут *Скрытый* (Hidden), вы не сможете просматривать их при помощи *Проводника*. Но лишь до тех пор, пока не укажете в установках *Проводника* другие значения. Чтобы изменить установки *Проводника*, откройте меню *Вид* и выберите *Свойства папки*. На экране появится одноименное диалоговое окно.

Щелкните на переключателе *Вид* и включите опцию *«не показывать скрытые файлы»*. Установка этой опции приведет к тому, что файлы и папки с атрибутом *Скрытый* (Hidden) не будут отображаться *Проводником*.

Сделайте невидимой вашу папку.

Сделайте невидимыми все папки диска D.

Возвратите все папки и файлы в прежнее состояние.

3. Применение программ-архиваторов для скрытия и защиты файлов.

Произведите архивацию нескольких файлов вашей папки с помощью программы WinZip или WinRar.

Откройте программу WinZip или WinRar.

Создайте архив: щелкните по кнопке *New*.

Выберите папку, где будет храниться архив и имя архива (с расширением .zip). Нажмите *OK*.

Откройте архив (пока пустой) и щелкните по кнопке *Add* (добавить файл в архив). В появившемся меню выберите файл, который вы будете архивировать, и щелчком по нему введите его имя. Нажмите *OK*.

4. Парольная защита архива.

Откройте архив, который вы создали.

Добавьте другой файл в архив.

Защитите архив паролем. Нажмите *OK*.

Запишите пароль.

Задание 6. Чтение и уничтожение удаленных файлов и исправленного текста

1. Программы Norton Unerase и Norton Wipeinfo.

Установите программы Norton Utilites, если они не установлены.

Удалите из своей папки ненужный вам файл. Очистите корзину.

Восстановите удаленный файл утилитой Norton Unerase программы Norton Utilites.

Уничтожьте этот восстановленный файл утилитой Norton Wipeinfo программы Norton Utilites.

2. Уничтожение удаленного и исправленного текста.

В процессе создания и редактирования текста вы можете его исправлять, в том числе удалять его фрагменты: слова, строки, абзацы. Эти удаленные фрагменты сохраняются в документе на диске.

Если вы хотите, чтобы удаленный текст не был сохранен в документе, нет необходимости просматривать его другой программой, достаточно выполнить следующие действия:

Сохраните исходный документ, который вы отредактировали.

Создайте новый документ (в меню *Файл* выберите команду *Создать*.

Возвратитесь к исходному документу.

Выделите весь документ (в меню *Правка* выберите команду *Выделить все*).

Скопируйте выделенный текст (в меню *Правка* выберите команду *Копировать*).

Откройте документ.

Вставьте скопированное содержимое в созданный документ.

Сохраните его.

Поскольку вы скопировали только то, что отображалось на экране в исходном документе, то новый документ не будет содержать ничего другого.

Сравните размеры старого и нового документа.

3. Поиск и удаление временных файлов вручную.

Папка, которую нужно проверить на предмет наличия бесполезных временных файлов, называется \WINDOWS\TEMP (включая все папки, вложенные в нее). В них могут находиться файлы с расширением .TMP, но могут встретиться и более экзотические, например, .DOC или HTML. Там же можно обнаружить файлы с изображениями (например, .JPG) или файлы без расширения. Большинство таких файлов имеет нулевую (0) длину. Имя типичного временного файла начинается с символа ~ *{тильда}*, например, ~wrdtemp. doc.

Можете просмотреть временные файлы резервных копий, созданных тем или иным приложением. Для этого достаточно после запуска приложения выбрать в меню *Файл* команду *Открыть*. В появившемся окне можно, как правило, обнаружить файлы с соответствующими названиями, например, ~document. doc. Такие файлы должны удаляться после завершения работы приложения, но иногда они остаются.

Для удаления таких файлов запустите *Проводник*. Переместитесь в каталог, содержащий файлы, подлежащие удалению. Для удаления файла щелкните на нем, затем нажмите клавишу *Delete* и подтвердите выполнение операции. Если требуется удалить несколько файлов, следует выделить их и нажать клавишу *Delete*. Для выделения нескольких файлов нажмите клавишу *Ctrl* и, удерживая ее нажатой, поочередно щелкайте на каждом файле. Можно щелкнуть на первом

файле, а затем, удерживая нажатой клавишу *Shift*, переместить выделение при помощи клавиш управления курсором.

4. Поиск и удаление файлов с расширением .bak: такое расширение имеют копии файлов.

Нажмите последовательно *Пуск* > *Найти* > *Файлы* и папки.

В появившемся меню в строке *Имя* наберите *.bak.

В строке *Где искать* установите место поиска, например, диск С.

Нажмите кнопку *Найти*. В окне появятся файлы с расширением .bak.

Нажмите последовательно *Правка* > *Выделить все*. Удалите файлы через контекстное меню.

5. Программы очистки диска.

Очистите диск утилитой cleanmgr.exe программы Windows.

Нажмите последовательно *Пуск* > *Программы* > *Стандартные* > *Служебные* > > *Очистка диска*.

В появившемся меню в строке выберите диск, на котором следует произвести очистку, например, диск С: и нажмите *ОК*.

Установите флажки тех файлов, которые нужно удалить и нажмите *ОК*.

Задание 7. Защита от вирусов

Установите на компьютере антивирусную программу Doctor Web (Norton Antivirus, Antiviral Toolkit Pro).

Установите параметры программы Doctor Web (Norton Antivirus, Antiviral Toolkit Pro).

Вылечите или удалите зараженные файлы.

Задание 8. Защита в сети Интернет

Проверьте безопасность посещаемого вами узла Web. (В обозревателе Internet Explorer нужно выбрать в меню *Сервис* пункт *Свойства обозревателя* и щелкнуть на вкладке *Безопасность*).

Просмотрите предысторию вашей работы в сети Интернет (кнопка *Журнал* или *Вид* > *Панели обозревателя* > *Журнал*). Удалите посещенные вами адреса URL.

Скройте поле *Адресная строка* браузера Internet Explorer через правую кнопку мыши.

Удалите временные файлы Интернета (В обозревателе Internet Explorer нужно выбрать в меню *Сервис* пункт *Свойства обозревателя*, щелкнуть на вкладке *Общие* и на кнопке *Удалить*).

Устраните файлы cookie (В обозревателе Internet Explorer нужно выбрать в меню *Сервис* пункт *Свойства обозревателя*, щелкнуть на вкладке *Безопасность* и на кнопке *Другой*).

Восстановите Адресную строку браузера и файлы cookie.

Задание 9. Самостоятельная разработка программы, практическая работа на компьютере

Разработайте программу, представляющую собой форму доступа к определенным информационным ресурсам на основе пароля.

Создайте файлы:

- первый тип, который требует пароль для открытия;
- второй тип, который не позволяет вносить изменения в файл.

Решите следующие ситуационные задачи.

Ситуация 1.

Ты общаешься в социальной сети со своими друзьями. Неожиданно от незнакомого тебе человека приходит сообщение: «Привет, у тебя отличные фото! Только у меня все равно круче! Жми скорее сюда!». Предлагается перейти по ссылке для просмотра фотографий. Как следует поступить в данной ситуации?

Ситуация 2.

Ты находишься в сети Интернет, изучаешь сайты с информацией, интересной для тебя. Вдруг наталкиваешься на сайт, который предлагает составить твой личный гороскоп. Ты переходишь по ссылке, отвечаешь на все предложенные вопросы. В конце опроса тебе предлагается ввести номер мобильного телефона. Какими будут твои действия? Почему?

Ситуация 3.

Тебе позвонил друг и сообщил, что увидел в сети Интернет сообщение о срочном сборе средств для больного ребенка. Деньги предлагается перевести на счет указанного мобильного телефона или на электронный кошелек. Твой друг настаивает на помощи ребенку. Какими будут твои действия? Почему?

Ситуация 4.

Во время общения в социальной сети тебе приходит сообщение: «Привет! Мы с тобой как-то виделись у наших общих друзей. Решил тебя найти в сетях. Классная у тебя страничка! Может пойдем вечером гулять?» Как ты поступишь в этой ситуации? Почему?

Контрольные вопросы:

1. С какими проблемами сталкивается человек в информационном обществе?
2. Что такое информационная безопасность?
3. Какие объекты нуждаются в обеспечении информационной безопасности?
4. Чем грозит нарушение информационной безопасности гражданам, частным организациям, государству?
5. Почему опасны компьютерные игры?
6. Что такое угроза информационной безопасности?
7. Какие существуют классификации угроз информационной безопасности?
8. Что такое компьютерный вирус?
9. Что такое политика безопасности?
10. Могут ли вредоносные программы украсть вашу переписку с друзьями?
11. Можно ли скачивать игры с неизвестных сайтов?
12. Можно ли открывать письма от неизвестного вам человека, если он предлагает перейти по определенной ссылке, чтобы посмотреть фотографии, картинки?
13. Нужно ли советоваться с родителями, если незнакомый человек предлагает совершить какие-либо действия (скачать игру, посмотреть видеоролик)?
14. Все ли сайты в Интернете безопасны?
15. Можно ли использовать сеть Интернет без всяких опасений?
16. Может ли общение в социальных сетях принести вам какой-нибудь вред?

Меры безопасности и правила сетевого этикета, выполнение практических заданий, отражающих реальные ситуации поведения в Сети и виртуальном общении (девиз «Сетевой этикет»)

Материал для ознакомления

Современный мир цифровых коммуникаций и Интернета изменил поведение людей и способы их взаимодействия. Онлайн-среда стала местом, где мы общаемся, делимся информацией, ищем новости, работаем и развлекаемся. Однако, как и в реальном мире, существуют правила и нормы, регулирующие поведение в Сети. Эти правила известны как сетевой этикет.

Сетевой этикет (сетикет или нетикет) — это набор принятых общепризнанных норм и правил поведения, которые помогают нам вести себя в онлайн-среде вежливо, уважительно и этично. Сетевой этикет включает в себя различные аспекты, такие как уважение к частной жизни, соблюдение авторского права, правильное использование электронной почты, социальных сетей и форумов, а также соблюдение правил безопасности и конфиденциальности данных.

Владение сетевым этикетом дает ряд важных преимуществ.

Во-первых, следование этикету способствует созданию гармоничной и приятной онлайн-среды. Сетевой этикет помогает предотвратить конфликты, споры и неприятные ситуации, которые могут возникнуть из-за неправильного поведения или неверного толкования сообщений. Он позволяет участникам сетевого взаимодействия чувствовать себя комфортно и безопасно.

Во-вторых, владение сетевым этикетом способствует улучшению качества коммуникации. Правильное использование сетевого этикета позволяет ясно и точно выражать свои мысли и идеи, быть внимательными к другим участникам диалога и уважать их право на собственное мнение. Это способствует более продуктивному обмену информацией, конструктивным дебатам и решению проблем.

Сетевой этикет является неотъемлемой частью онлайн-жизни. Он помогает вести себя уважительно, этично и безопасно, создавая приятную и продуктивную сетевую среду для всех участников.

Интернет — огромное пространство для общения, обмена информацией и взаимодействия с другими людьми. Однако, чтобы поддерживать здоровую и позитивную онлайн-среду, важно придерживаться правил поведения. Ниже приведены правила, которые помогут этично взаимодействовать с другими пользователями Интернета.

- ✓ Будьте уважительны и вежливы. Уважайте других участников Интернета так же, как вы хотели бы, чтобы уважали вас. Избегайте грубости, оскорблений и унизительных комментариев. Помните, что за экраном находятся реальные люди, имеющие свои чувства и права.
- ✓ Будьте осмотрительны при публикации контента. Прежде чем делиться информацией или контентом в Интернете, обязательно проверьте его достоверность и релевантность. Избегайте распространения ложных или заведомо неправильных данных. Помните, что ваши слова и действия могут иметь долгосрочные последствия.
- ✓ Думайте перед тем, как писать. Прежде чем отправить сообщение или комментарий, обдумайте его содержание и тон. Учтите, что написанное в Интернете может быть воспринято по-разному. Избегайте использования

«капса» (написания большими буквами), поскольку его можно интерпретировать как крик или агрессию.

- ✓ Учитесь отличать факты от мнений. В Интернете множество мнений и разных точек зрения. При взаимодействии с другими участниками отличайте факты от мнений и будьте открыты к различным взглядам. Уважайте право каждого на мнение, даже если оно отличается от вашего.
- ✓ В Интернете возможны разногласия и споры. Будьте готовы к конструктивному диалогу и компромиссам, выслушивайте других и старайтесь найти общие решения. Избегайте жесткости, наступательности или стремления к победе в каждом споре.
- ✓ Будьте осторожны в обращении с личной информацией. Не теряйте бдительности при раскрытии личной информации в Интернете. Избегайте предоставления конфиденциальных данных без необходимости. Оценивайте возможные риски и принимайте меры для защиты своей онлайн-приватности.
- ✓ Будьте терпимы к различиям. Интернет объединяет людей разных культур, с разными мнениями и взглядами на жизнь. Будьте открыты к различиям. Избегайте перехода на личности и пишите конструктивные сообщения.

Главное о сетевом этикете

Сетевой этикет — набор принятых общепризнанных норм и правил поведения в онлайн-среде. Он необходим для поддержания взаимопонимания и уважительного общения в онлайн-среде, помогает предотвращать конфликты, снижает риск неприятных ситуаций и позволяет создать основу для продуктивного взаимодействия и успешного достижения целей в онлайн-мире.

Главные правила сетевого этикета:

- ✓ быть вежливым и уважительным к другим участникам, избегать грубости и оскорблений;
- ✓ соблюдать приватность, не распространять чужую личную информацию;
- ✓ быть осмотрительным с контентом, проверять его достоверность и избегать распространения дезинформации;
- ✓ уважать интеллектуальную собственность, не нарушать авторские права;
- ✓ аккуратно подбирать слова, избегать нецензурных выражений.

Практическая работа «Сетевой этикет» (в парах)

Цель: сформировать практические навыки сетевого этикета.

Задачи:

- сформировать умение правильно оформлять электронное письмо официального характера;
- сформировать умение составлять «Регламент мероприятий»;
- сформировать умение отвечать на грубую речь в электронных письмах.

Практические, ситуационные задания

Задание 1.

Учащийся исполняет роль менеджера крупной компании. Ему дали следующее задание.

Грамотно написать деловое письмо партнерам по бизнесу, и отправить его на определенный электронный адрес: учителя или партнера по выполнению задания, другого учащегося.

Задание конкретизировал директор, собираясь на очередную деловую встречу:

«Отправишь письмо о завтрашнем совещании! Они мне все завтра нужны утром! Без опозданий! В 8:00 уже начну слушать доклады. Кстати, пригласи эксперта по продажам Миронова и включи его в список выступающих. Пусть все собираются в конференц-зале. Веронике я сказал, технику она подготовит. Заседание будет идти долго, поэтому вставь в расписание кофе-паузу. Начнем с доклада Петрова о продажах в прошлом квартале, затем отведи время для нашего инвестора Григория Александровича Сафонова, потом уж бухгалтерия подключится, дальше я, ну и эксперт по продажам. Да, чуть не забыл, после совещания приедет автобус, позвони на объект, уточни все ли у них готово, потому что после совещания все поедут смотреть новый ТЦ: экскурсия, все дела, ну и доклад прораба. Регламент для всех: до 25 минут для доклада».

Задание 2.

Корректно ответить на угрозы заказчика, объяснить ситуацию и быть непреклонным в своих доводах.

Учащийся в роли директора одного из предприятий застройщиков.

Организация выиграла тендер на строительство детской площадки одного из микрорайонов. Аванс на счет организации ушел, бумаги все подписаны, однако объект «заморозили» органы пожарной безопасности. Вашей вины в том нет, полностью вина лежит на заказчике (Степане Игоревиче).

Однако, вам приходит гневное письмо от заказчика:

«ГДЕ ГОТОВЫЙ ОБЪЕКТ ПО УЛИЦЕ МОЛДАВСКОЙ? Все сроки уже прошли!!!! Если ВЫ, уважаемые, не сдадите нам объект, в четверг на следующей неделе, как это было ОГОВОРЕНО в ДОГОВОРЕ, ТО НАШ РАЗГОВОР будет продолжаться уже в суде!»

Практические задания, отражающие проблему информационно-психологической безопасности (девиз: «Подводные камни Интернета»)

Материал для ознакомления

Интернет — это современная среда взаимодействия людей. В ней новое звучание приобретают многие правила и закономерности, известные людям с давних времен.

Но современный Интернет — это не только обширная, но и настраиваемая среда обитания! В Интернете хорошо тому, кто может обустроить в нем собственное пространство и научиться управлять им. Можно записывать собственные впечатления в блог, создавать галереи своих фотографий и видео, включать в друзья людей, которым доверяете. Тогда вместо бессмысленного блуждания по Сети интернет-общение будет приносить пользу.

В ходе выполнения заданий необходимо решить следующие ситуационные задачи и представить результат в виде презентации:

«Какие опасности подстерегают человека при посещении Интернета и общении в социальных сетях?»

«Подводные камни, которые можно встретить, путешествуя по Сети: интернет-зависимость; вредоносные и нежелательные программы; психологическое

воздействие на человека через Интернет; материалы нежелательного содержания; интернет-мошенники».

«Какие опасности и киберугрозы подстерегают нас в сети Интернет?»

«Какие подводные камни можно встретить, путешествуя по Сети?»

Тема 2. Индивидуальные проекты в сфере информационной безопасности (10 часов)

Мини-проект «Шифрование информации»

Перед выполнением проекта необходимо изучить следующие теоретические вопросы:

История криптографии. Криптография в Древнем мире. Тайнописи. Криптография от Средних веков до Нового времени. Криптография Первой мировой войны. Криптография Второй мировой войны. Современная криптография.

Практическая работа

Выполнение индивидуальных мини-проектов по криптографии (шифрованию).

План работы над проектом

1) Выбор темы проекта.
2) Реализация проекта.
3) Презентация проекта.
4) Анализ работы над проектом.

В рамках общей тематики «Шифрование информации» вам предлагаются следующие индивидуальные темы:

Создание собственного шифра

Задание. Изучите теоретические аспекты шифрования, найдите области его применения, рассмотрите сильные и слабые стороны шифра. Обязательно подготовьте презентацию.

Самостоятельная работа: нахождение материала о способах шифрования, рассмотрение теории шифрования и расшифровки файла. Оценка сложности алгоритма, подготовка презентации проекта. Проектирование собственного алгоритма шифрования.

Разработка программного средства для зашифровки и расшифровки сообщения, файла и т. д.

Мини-проект «Угрозы безопасности и методы их устранения»

Задание. Рассмотреть типы и виды угроз и предложить методы их устранения.

Мини-проект «Средства управления криптографическими ключами»

Задание. Рассмотреть теорию и практику создания криптографических ключей.

Мини-проект «Мир без Интернета»

Задание. Изучите основы работы в глобальных информационных сетях, оцените практическое применение Интернета.

План работы над проектом

1. Реализация проекта.
2. Презентация проекта.
3. Анализ работы над проектом.
4. Содержательная часть проекта должна включать следующие вопросы:

Цель проекта:

- выяснить как изменится мир, если убрать Интернет;
- определить, чем же так полезен Интернет и почему без него не могут обойтись люди.

Задачи проекта:

- изучить и представить зарождение Интернета;
- выяснить путем опроса, к чему приведет отсутствие Интернета в наше время.

Основные вопросы, которые следует рассмотреть в процессе выполнения проекта:

1. Что такое Интернет?
2. Как «зародился» Интернет?
3. Какова география Интернета?
4. Какие сервисы предоставляет Интернет?
5. Что будет с миром, если пропадет Интернет?
6. Каким вы представляете мир без Интернета?
7. Что будет с человечеством, если Интернет исчезнет?
8. Возможно ли прекратить существование Интернета?

Примерная тематика проектной деятельности (по выбору):
«Зарождение глобальной сети Интернет».
«Роль Интернета в жизни человека».
«Интернет: зло или благо?»
«Вся правда о социальных сетях».
«Альтернатива Интернету».
«Полезные ресурсы Интернета».

Мини-проект «Информационное общество»

Материал для ознакомления

Информационное общество — новая историческая фаза развития цивилизации, в которой главными продуктами производства являются информация и знания. Основные черты информационного общества:

- увеличение роли информации и знаний в жизни общества;
- возрастание числа людей, занятых в сфере информационных и коммуникационных технологий;
- рост доли информационных продуктов и услуг в валовом внутреннем продукте;
- широкомасштабное использование ИКТ во всех сферах социально-экономической, политической и культурной жизни общества;
- создание глобального информационного пространства;
- развитие информационной экономики, электронного правительства, электронных социальных сетей.

Совокупность всей информации, накопленной человечеством в процессе развития науки, культуры, образования и практической деятельности людей, называют информационными ресурсами. Государственные информационные ресурсы используются для решения задач государственного управления, обеспечения прав и безопасности граждан, поддержки социально-экономического развития страны, развития культуры, науки, образования.

Информационные ресурсы — отдельные документы и отдельные массивы документов, в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

Информационные ресурсы общества можно рассматривать как знания, накопленные человечеством и материализованные в виде документов, баз данных, баз знаний, алгоритмов, компьютерных программ, произведений искусства, литературы и науки.

Информационные ресурсы можно классифицировать следующим образом:

- библиотечные ресурсы;
- архивные ресурсы;
- научно-техническая информация;
- правовая информация и информация государственных структур;
- отраслевая информация;
- финансовая и экономическая информация;
- информация о природных ресурсах и т. д.

Информационные ресурсы признаются одним из важнейших видов ресурсов в любой стране. В наиболее развитых странах они являются объектом особого внимания.

Сейчас активно идет процесс снижения ценности материального продукта, но повышается ценность информации. В современном обществе информация становится ценным продуктом.

Информационный продукт — информация всех видов, программные продукты, базы данных, представленные в форме товара, т. е. созданные с целью продажи за деньги или обмена на другие продукты.

Информационный продукт — это уникальный показатель эпохи всеобщей автоматизации и информатизации и имеет ряд определенных отличий от материального продукта. Так, любой информационный продукт обладает качеством, которое присуще информации в целом — он не подвержен амортизации, физическому износу. Вы можете неоднократно использовать информационный продукт, и он не потеряет в качестве и уникальности. Для примера: многократное воспроизведение фильма никак не повлияет на его содержание. Фильм не становится хуже с каждым просмотром. Но следует сказать, что информационный продукт подвержен так называемому моральному устареванию. Информация, которая была актуальной еще вчера, может потерять всю свою значимость и востребованность сегодня. Также показательным свойством информационного продукта является то, что расходы на его изготовление, как правило, в разы превосходят дальнейшие расходы на его тиражирование. Написать уникальную работу один раз всегда сложнее, чем затем размножить ее на тысячи экземпляров. Немаловажное свойство информационного продукта — его адресность. В зависимости от группы потребителей производитель выбирает форму и способ изготовления будущего информационного продукта. Так, публикация научной работы в профессиональном сообществе будет отличаться от способа популяризации той же научной идеи для учащихся. Информационный продукт имеет свойство универсальности: может представлять ценность для разных областей применения, использоваться с разными целями в разных проектах.

Информационные продукты распространяются посредством информационных услуг.

Информационная услуга — получение и предоставление в распоряжение пользователя информационных продуктов.

В узком смысле информационная услуга часто воспринимается как услуга, получаемая с помощью компьютеров, хотя на самом деле это понятие намного шире.

При предоставлении услуги заключается соглашение (договор) между двумя сторонами — предоставляющей и использующей услугу. В договоре указываются срок ее использования и соответствующее этому вознаграждение.

Перечень услуг определяется объемом, качеством, предметной ориентацией по сфере использования информационных ресурсов и создаваемых на их основе информационных продуктов.

Как и при использовании традиционных видов ресурсов и продуктов, люди должны знать: где находятся информационные ресурсы, сколько они стоят, кто ими владеет, кто в них нуждается, насколько они доступны. Ответы на эти вопросы можно получить, если существует рынок информационных продуктов и услуг.

Рынок информационных продуктов и услуг (информационный рынок) — система экономических, правовых и организационных отношений по торговле продуктами интеллектуального труда на коммерческой основе.

В пространстве информационного рынка можно выделить пять секторов:

1) научно-техническая продукция в виде проектных, технологических, методических разработок по разным отраслям;
2) объекты художественной культуры в виде текстовой, визуальной и аудиопродукции;
3) услуги образования: все виды обучения;
4) управленческие данные и сообщения: политическая и хозяйственная информация, статистические данные, данные о рыночной ситуации, рекламные сообщения, оценки и рекомендации по принятию решений;
5) бытовая информация: сообщения общего характера, сведения о потребительском рынке, сведения о рынке труда.

По мере продвижения к информационному обществу все большие возможности, связанные с использованием информационных и коммуникационных технологий, появляются в сфере образования, способствуя повышению его доступности и качества, созданию системы непрерывного образования.

В современном обществе имеется огромное количество разнообразной информационной техники (компьютеры, телефоны, телевизоры, факсы и пр.). Появляется множество профессий, связанных с поиском, хранением, преобразованием информации. Информация становится определяющим ресурсом экономического и общественного развития. Ошибочно информатизация понимается исключительно лишь как процесс внедрения современных компьютерных, информационных технологий в жизнь человека и общества на базе новейшей компьютерной, телекоммуникационной техники и Интернета. В чем же суть и смысл процесса информатизации? Информатизация — это процесс овладения информацией как ресурсом управления и развития с помощью средств информатики с целью создания информационного общества и на этой основе — дальнейшего продолжения прогресса цивилизации.

Индивидуальные мини-проекты по теме «Информационное общество»

План работы над проектом

1. Реализация проекта.
2. Презентация проекта.
3. Анализ работы над проектом.

Содержательная часть проекта должна включать следующие вопросы:

Цель проекта: раскрыть содержание понятия «информационное общество».

Задачи проекта:

- изучить и проанализировать основные тенденции развития информационного общества;
- научиться выделять особенности формирования информационных ресурсов общества;
- рассмотреть вопросы правил поведения в социальных сетях и системах обмена сообщениями;
- дать характеристики и пути развития информационного общества, информационных ресурсов, продуктов, услуг;
- охарактеризовать правила поведения в социальных сетях и системах обмена сообщениями;
- определить и охарактеризовать соотношение информационных ресурсов и услуг с секторами информационного рынка;
- дать характеристику информационно-образовательной среды своего учреждения образования;
- проанализировать принципы построения информационного общества, характеризовать возможности социальных сетей.

Тематика проектной деятельности может быть расширена следующими проектными исследованиями:

«Информационно-телекоммуникационная инфраструктура информационного общества и услуги, оказываемые на ее основе».

«Формирование информационной среды предприятия (учреждения)».

«Безопасность в информационном обществе».

«Информационное государство».

«Искусственный интеллект, виртуальная реальность и виртуальная личность».

Тема 3. Выполнение группового проекта (15 часов)

Инструкция: в процессе выполнения проекта организуется групповая деятельность по выполнению поставленных задач совместного проекта: обсуждение возможных вариантов решения поставленных задач, сравнение возможных стратегий, выбор оптимальной стратегии, совместное составление плана действий, распределение обязанностей.

Деятельность по выполнению проекта сопровождается выбором программного решения с внесением при необходимости изменений, совместное выполнение каждого этапа проекта с анализом полученных результатов.

Итогом группового проекта является презентация полученных результатов и защита проекта группой.

Этапы работы над проектом

1. Введение в проектную деятельность.
2. Определение и утверждение тематики проекта.
3. Составление графика работы над проектом.
4. Подбор и анализ источников.
5. Анализ и контроль процесса выполнения проекта (консультации).
6. Контроль за оформлением проекта.
7. Организация и проведение предзащиты проекта.
8. Контроль за доработкой проекта.
9. Защита проекта.
10. Подведение итогов работы.

Примерная тематика проектов: «Обеспечение информационной безопасности в нашей школе», «Информационная безопасность: миф или реальность?», «Как обеспечить личную безопасность в сети Интернет?», «“Умный дом” и как его защитить от вторжения».

Проект «Обеспечение информационной безопасности в нашей школе». Материал для ознакомления

В настоящее время Интернет стал неотъемлемой частью нашей повседневной жизни. Использование Интернета в образовательных учреждениях и дома расширяет информационное образовательное пространство учащегося и позволяет повысить эффективность обучения. Доступ учащихся к информационным ресурсам сети Интернет дает возможность пользоваться основным и дополнительным учебным материалом, необходимым для обучения в школе, выполнять домашние задания, самостоятельно обучаться. Благодаря таким ресурсам у учащихся появляется возможность узнавать о проводимых олимпиадах, конкурсах, и принимать в них активное участие. Использование Интернета в работе образовательного учреждения достаточно обширно. Это:

- использование электронной почты;
- поиск в сети нужной информации;
- создание собственных школьных веб-страниц;
- рассылка и/или съем материалов (нормативных документов, информации об олимпиадах и конкурсах и т. п.);
- обмен опытом;
- ответы на типичные вопросы;
- получение («скачивание») небольших обучающих программ по разным предметам;
- совместные проекты учащихся и учителей, в том числе разных школ.

Система информационной безопасности учреждения образования должна не только обеспечивать сохранность баз данных и содержащихся в них массивов конфиденциальных сведений, но и гарантировать невозможность доступа в стены школы любой пропаганды, как незаконного характера, так и безобидной, но предполагающей воздействие на сознание учащихся.

В понятие информационной безопасности учреждения входит система мер, направленная на защиту информационного пространства и персональных данных от случайного или намеренного проникновения с целью хищения каких-либо данных или внесения изменений в конфигурацию системы. Вторым аспектом понятия станет защита образовательного процесса от любых сведений, носящих характер запрещенной законом пропаганды или любых видов рекламы.

В составе массивов охраняемой законом информации, находящейся в распоряжении учреждения образования, можно выделить три группы:

1) персональные сведения, касающиеся учащихся и преподавателей;
2) оцифрованные архивы;
3) ноу-хау образовательного процесса, носящие характер интеллектуальной собственности и защищенные законом.

Все эти сведения могут стать не только объектом хищения. Намеренное проникновение в них может нарушить сохранность оцифрованных книг, уничтожить хранилища знаний, внести изменения в код программ, используемых для обучения.

Необходимо гарантировать сохранение данных в целостности и неприкосновенности и обеспечение их:

- доступности в любое время для любого авторизированного пользователя;
- защиты от любой утраты или внесения несанкционированных изменений;
- конфиденциальности, недоступности для третьих лиц.

Угрозы информационной безопасности в учреждении образования

Особенностью угроз становится не только возможность хищения сведений или повреждение массивов какими-либо сознательно действующими хакерскими группировками, но и сама деятельность подростков, намеренно, по злому умыслу или ошибочно способных повредить компьютерное оборудование или внести вирус. Выделяются четыре группы объектов, которые могут подвергнуться намеренному или ненамеренному воздействию:

1) компьютерная техника и другие аппаратные средства, которые могут быть повреждены в результате механического воздействия, вирусов, по иным причинам;
2) программы, используемые для обеспечения работоспособности системы или в образовательном процессе, которые могут пострадать от вирусов или хакерских атак;
3) данные, хранимые как на жестких дисках, так и на отдельных носителях;
4) сам персонал, отвечающий за работоспособность информационных систем.

Угрозы, направленные на повреждение любого из компонентов системы, могут носить как случайный, так и преднамеренный характер. Среди угроз, не зависящих от намерения персонала, учащихся или третьих лиц, можно назвать:

- любые аварийные ситуации, например, отключение электроэнергии или какое-либо стихийное бедствие;
- ошибки персонала;
- сбои в работе программного обеспечения;
- выход техники из строя;
- проблемы в работе систем связи.

Все эти угрозы информационной безопасности носят временный характер, предсказуемы и легко устраняются действиями сотрудников и специальных служб.

Намеренные угрозы информационной безопасности носят более опасный характер и в большинстве случаев их невозможно предвидеть. Их виновниками могут оказаться учащиеся, служащие, конкуренты, третьи лица с намерением на совершение киберпреступления. Для подрыва информационной безопасности такое лицо должно иметь высокую квалификацию в отношении принципов работы информационных систем и программ. Наибольшей опасности подвергаются

информационные сети, компоненты которых расположены отдельно друг от друга в пространстве. Нарушение связи между компонентами системы может привести к полному подрыву ее работоспособности. Важной проблемой может стать нарушение авторских прав, намеренное хищение чужих разработок. Информационные сети редко подвергаются внешним атакам с целью воздействия на сознание, но и это не исключено. И самой серьезной опасностью станет использование школьного оборудования для вовлечения учащегося в криминал и терроризм.

План работы над проектом

1. Реализация проекта.
2. Презентация проекта.
3. Анализ работы над проектом.

Содержательная часть проекта должна включать следующие вопросы:

Цель проекта:

- формирование безопасной информационно-образовательной среды школы;
- обеспечение информационной безопасности учащихся, использующих Интернет в различных целях, в том числе образовательных;
- пропаганда и организация безопасного поведения в сети Интернет.

Задачи:

- внести предложения по организация технического контроля информационной безопасности;
- внести предложения по участию в проекте учителя (классного руководителя) по использованию образовательных ресурсов Интернета;
- обеспечить создание условий поддержки информационной безопасности учащихся, использующих Интернет в образовании;
- создать сайт учреждения образования;
- провести опрос и анкетирование среди учащихся и их родителей;
- спроектировать структуру информационной безопасности.

Примерная структура и содержание проекта

- Введение.
- Теоретические основы обеспечения информационной безопасности в учреждениях образования.
- Практический подход к обеспечению информационной безопасности в учреждении образования.
- Анализ обеспечения информационной безопасности в нашей школе.
- Проблемы обеспечения информационной безопасности в нашей школе.
- Проектные предложения по усовершенствованию обеспечения информационной безопасности в нашей школе.
- Заключение.
- Список использованной литературы.
- Приложения (проекты аппаратно-программных решений, проекты Положений и нормативных документов).

Проект «Информационная безопасность: миф или реальность?»

Материал для ознакомления

Информационная безопасность — это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий

естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений.

Информационная безопасность — это и защита конфиденциальности, целостности и доступности информации.

Целостность: неизменность информации в процессе ее передачи или хранения.

Доступность — свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц.

Конфиденциальность: свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц:

- как состояние окружающей среды или объекта, в котором существует возможность причинить им существенный ущерб или вред путем оказания воздействия на информационную сферу объекта;
- как свойство объекта, характеризующееся способностью наносить существенный ущерб другому объекту путем оказания воздействия на его информационную сферу. В соответствии с этим информационная безопасность — это состояние объекта, когда ему путем воздействия на его информационную сферу не может быть нанесен существенный ущерб или вред;
- свойство объекта, характеризующее его способность не наносить существенного ущерба какому-либо объекту путем оказания воздействия на информационную сферу этого объекта.

Информационная безопасность личности — это состояние человека, в котором его личности не может быть нанесен существенный ущерб путем оказания воздействия на окружающее информационное пространство.

Информационная безопасность общества — это состояние общества, в котором ему не может быть нанесен существенный ущерб путем воздействия на его информационную сферу. В ее основе — безопасность индивидуального, группового и массового сознания граждан при наличии информационных угроз, к которым в первую очередь следует отнести информационно-психологическое воздействие. Действие этих угроз может вызывать психоэмоциональную и социально-психологическую напряженность, искажение нравственных критериев и норм, морально-политическую дезориентацию и, как следствие, неадекватное поведение отдельных лиц, групп и масс людей. В результате таких воздействий возможны глубокие трансформации индивидуального, группового и массового сознания, негативные изменения морально-политического и социально-психологического климата в обществе.

Информационная безопасность государства — это состояние государства, в котором ему не может быть нанесен существенный ущерб путем оказания воздействия на его информационную сферу. Обеспечение информационной безопасности государства неразрывно связано с обеспечением национальной безопасности.

Технологии защиты данных основываются на применении современных методов, которые предотвращают утечку информации и ее потерю. Сегодня используется шесть основных способов защиты:

1) препятствие;
2) маскировка;

3) регламентация;
4) управление;
5) принуждение;
6) побуждение.

Методы защиты информации: аутентификация и идентификация.

Аутентификация представляет собой проверку того, является ли тот субъект/объект тем, за кого пытается себя выдать.

Идентификация представляет собой присвоение субъекту или объекту уникального образа или имени.

Создание базовой системы зашиты информации в информационных системах (ИС) основывается на следующих принципах.

Комплексный подход к построению системы защиты при ведущей роли организационных мероприятий. Он означает оптимальное сочетание программных аппаратных средств и организационных мер защиты.

Полнота контроля и регистрации попыток несанкционированного доступа, т. е. необходимость точного установления идентичности каждого пользователя и протоколирования его действий для проведения возможного расследования, а также невозможность совершения любой операции обработки информации в ИС без ее предварительной регистрации.

Обеспечение надежности системы защиты, т. е. невозможность снижения ее уровня при возникновении в системе сбоев, отказов, преднамеренных действий нарушителя или непреднамеренных ошибок пользователей и обслуживающего персонала.

Обеспечение контроля за функционированием системы защиты, т. е. создание средств и методов контроля работоспособности механизмов защиты.

«Прозрачность» системы защиты информации для общего, прикладного программного обеспечения и пользователей ИС.

Экономическая целесообразность использования системы защиты. Это выражается в том, что стоимость разработки и эксплуатации систем защиты информации должна быть меньше стоимости возможного ущерба, наносимого объекту в случае разработки и эксплуатации ИС без системы защиты информации.

Полностью защищенный компьютер — это тот, который стоит под замком в бронированной комнате в сейфе, не подключен ни к какой сети (даже электрической) и выключен. Такой компьютер имеет абсолютную защиту, однако использовать его нельзя, так что в этом примере не выполняется требование доступности информации. «Абсолютности» защиты мешает не только необходимость пользоваться защищаемыми данными, но и усложнение защищаемых систем.

Специалисты не зря говорят: «Компьютерная защита — это постоянная борьба на два фронта: с глупостью пользователей и с интеллектом хакеров». Как правило, встречаются три варианта:

1) некомпетентность пользователей;
2) действия инсайдеров;
3) безалаберность системных администраторов.

Многие эксперты именно некомпетентность пользователей считают главной угрозой безопасности. Персональных компьютеров на рабочих местах становится все больше, и, соответственно, опытных пользователей (в процентном отношении) — все меньше. Уже классической стала проблема так называемых «слабых» паролей. Малоопытные пользователи для лучшего запоминания выбирают легко угадываемые

пароли либо используют один и тот же пароль для различных служб и сервисов. Причем проконтролировать сложность пароля невозможно, и единственным выходом часто становится принудительное назначение паролей системным администратором.

«Абсолютности» защиты мешает не только необходимость пользоваться защищаемыми данными, но и усложнение защищаемых систем. Использование постоянных, не развивающихся механизмов защиты опасно, и этому есть множество причин. Кроме того, нельзя забывать о развитии и совершенствовании средств нападения. Техника так быстро меняется, что трудно определить, какое новое устройство или программное обеспечение, используемое для нападения, может обмануть вашу защиту. Извечное соревнование брони и снаряда продолжается.

План работы над проектом

1. Реализация проекта.
2. Презентация проекта.
3. Анализ работы над проектом.

Содержательная часть проекта должна включать следующие вопросы:

Гипотеза проекта: должны ли мы знать способы защиты от интернет-преступности для обеспечение своей информационной безопасности?

Задачи проекта:

- познакомиться с литературой и интернет-источниками на данную тему;
- отработать и выстроить нужный материал, провести его анализ;
- выяснить, существенна ли проблема информационной безопасности среди учащихся, проведя социальный опрос и проанализировав его результаты;
- разработать рекомендации по защите и утечке информации;
- обобщить материал и оформить результаты.

Методы исследования:

- исследование научной литературы;
- сбор материалов исследования;
- анкетирование;
- обобщение полученных результатов.

Для выполнения проекта формируются группы из состава учащихся класса с условными «никами».

- Информационная:
  подбирает и оформляет материал по вопросам:
  информационные ресурсы общества;
  информационная свобода личности;
  информационный потенциал общества;
  информационное неравенство.
- Милитаристская:
  подбирает и оформляет материал по вопросам:
  информационная угроза;
  информационная война;
  информационное оружие.
- Юридическая:
  подбирает информацию для освещения правовых аспектов информационной безопасности в мире;
  изучает законодательство по вопросам информационной безопасности.

- Экономическая:
  подбирает информацию и освещает вопросы финансового ущерба от нарушений в сфере информационной безопасности.
- Аналитическая:
  на основе анализа традиционных и нетрадиционных источников информации составляет практические советы по защите информации разного характера: личной, деловой, государственной.

Выполнение проекта сопровождается решением следующих ситуационных задач:

- Информационная безопасность «облаков». Миф или реальность? Развеять мифы:
  - ✓ миф первый: ИТ-безопасность внутри организации обеспечена более надежно, чем в облаке;
  - ✓ миф второй: данные из облака похитить проще чем изнутри организации.
- Изучить основные риски облачных сервисов и рекомендации по их снижению.
- Реальность, похожая на миф: простая электронная подпись больше, чем коды!
- Чистый и безопасный код: миф или реальность?
- Кибервойна: миф или реальность?
- Безопасность в облаке: мифы и реальность. Обеспечение безопасности и безопасность как сервис.
- Информационные войны: миф или реальность?
- Защита персональных данных: миф или реальность? Кто и зачем собирает ваши личные данные?

Проект «Как обеспечить личную безопасность в сети Интернет?»

Материал для ознакомления

В современном мире всех окружает большое количество информации. Есть разные источники ее получения, но все чаще мы получаем ее не из книг и журналов, а из Интернета. Сегодня Интернет играет большую роль в жизни человека, а также оказывает огромное влияние на него.

Пользователей Интернета с каждым годом становится все больше, в том числе и среди учащихся, активно покоряющих Интернет, возраст которых постоянно молодеет. В правильном использовании Интернета важно определиться с тем, что можно и чего нельзя делать, каким рискам мы подвергаемся и как их избежать. Ведь в Интернете не только много полезной информации, но есть и такая, которая может нас обидеть, оскорбить, нанести психологическую травму. В ходе использования Интернета возникает вопрос «Все ли мы знаем о правилах безопасного поведения в сети Интернет и соблюдаем ли их?». Поэтому тема «Как обеспечить личную безопасность в сети Интернет?» и стала проектным заданием.

Цель проекта: овладение учащимися навыками безопасной работы в сети Интернет.

Задачи проекта:

- исследовать интересы учащихся в сети Интернет, их представления об информационной безопасности;
- познакомить с основами безопасной работы компьютера, научить их приемам безопасного поиска информации в сети Интернет;

- разработать памятку безопасной работы на компьютере, безопасного поиска информации в сети, безопасного общения в социальных сетях.

План действий по реализации проекта

1. Организация и проведение анкетирования с целью выявления интересов учащихся в сети Интернет, их представления об информационной безопасности.
2. Обсуждение результатов анкетирования.
3. Представление проекта памятки по безопасной работе в сети Интернет.

Проект «“Умный дом” и как его защитить от вторжения»

Материал для ознакомления

«Умный дом» — это единая система управления и контроля комфортом и безопасностью дома и его обитателей. Она контролирует не только целостность инженерных систем, но сохранит дом от визита непрошенных гостей. Системы безопасности включают охранно-пожарную сигнализацию, видеонаблюдение внутри дома, видеонаблюдение за участком, видеодомофон, охрану периметра.

Пожары, неисправности в системах подачи воды и несовершенные системы охраны становятся причиной серьезных материальных потерь. Как может обезопасить жизнь «умный дом»? Его система безопасности направлена на обеспечение инженерной и личной безопасности.

Инженерная безопасность

Система «умный дом» обеспечивает:

- защиту от протечек;
- защиту от короткого замыкания в электросети;
- защиту от возгораний (датчик задымления);
- автономное энергоснабжение (дизель-генератор);
- автоматическую систему пожаротушения;
- аварийную сигнализацию для вызова сервисных служб.

Тем самым системы безопасности предназначены обеспечить безопасность дома, защитить от любых чрезвычайных ситуаций. Сюда входят: защита от вторжения с помощью камер видеонаблюдения, автоматизации дверей, ворот, рольставен, охранной сигнализации, предотвращение аварийных ситуаций. Оставленные включенными утюг, щипцы или духовка будут вовремя выключены, а в случае любого возгорания или задымления сработает пожарная сигнализация. О протечках воды или газа система сразу же уведомит хозяина и соответствующие службы.

Личная безопасность и здоровье человека

Система «умный дом» обеспечивает:

- контроль целостности периметра (двери и окна);
- имитацию присутствия хозяев;
- автоматизированный контроль доступа в помещение;
- видеонаблюдение за прилегающей территорией;
- автоматическое освещение территории при проникновении;
- управление защитными жалюзи;
- возможность вызова вневедомственной охраны;
- получение картинки с любой камеры видеонаблюдения через Интернет;

- предотвращение ситуаций, угрожающих здоровью человека: защита от пожара, утечек газа и другое;
- необходимый комфорт и безопасность для обеспечения оптимального ухода за проживающими в доме.

Система «умный дом» обеспечивает комфорт и удобство использования благодаря применению интеллектуальных замков, систем освещения, интегрированной бытовой техники в общую интернет-систему. В то же время возникает угроза кибератак. У современных преступников отпадает необходимость вламываться в дом с помощью отмычек, ведь можно дистанционно вмешаться в работу дома, чтобы получить массу сведений и открыть замки.

Главная проблема интеллектуальных устройств и высокотехнологичных помещений — возможные кибератаки. Система безопасности должна учитывать перспективы масштабирования и быть готовой к взломам.

Сегодня для дистанционного управления «умным домом» применяется обычный смартфон. Защита дома будет складываться из комплекса мероприятий для устройств управления (компьютер, смартфон, мобильные приложения) и каждого элемента, имеющего выход в сеть Интернет.

«Умный дом» — зачем его защищать?

Привлекательны ли устройства «умного дома» для хакеров? Да.

Почему «умные» вещи пользуются все большим спросом у хакеров? Прежде всего, потому что в их памяти хранятся бесчисленные объемы данных. Даже такие неприметные гаджеты, как «умные» холодильники или духовки, содержат информацию о своих пользователях, которые иногда делятся ею, независимо от потенциальных угроз.

Какую информацию могут собирать устройства интернета вещей:

- планы домов (в случае интеллектуальных роботов-уборщиков);
- информацию о состоянии здоровья пользователей (собираемая, например, «умными» часами);
- данные о предпочтениях в еде и покупках (собранные «умными» холодильниками);
- контент, собираемый камерами наблюдения.

Производители «умных» устройств не всегда могут обеспечить должный уровень безопасности в своих гаджетах. Это связано с тем, что, в отличие от домашних компьютеров или смартфонов, большинство интеллектуальных устройств имеют относительно менее совершенные процессоры и программное обеспечение.

Они могут управлять подключением к сети и хранить необходимые данные, но у них нет вычислительной мощности, которая требует сложного шифрования или других превентивных (защитных) мер.

Некоторые производители интеллектуальных решений также известны тем, что слишком рано размещают свои изделия на рынке (то есть без надлежащего тестирования) или не предоставляют соответствующую дозу информации о безопасности в своих инструкциях по применению.

Сами владельцы таких устройств тоже иногда не в курсе, что подключают их, например, к незащищенным домашним сетям. Все это делает «умные» гаджеты чрезвычайно привлекательной питательной средой для хакеров. «Умный дом» можно довольно легко взломать.

Часто разработчики не уделяют достаточного внимания безопасности создаваемых продуктов. Например, известен случай, когда исследователь информационной безопасности смог найти ссылку на интерфейс управления системой «умного дома» прямо в Google. Страница не была защищена паролем, так что он получил возможность управления всеми умными системами, а также узнал адрес дома и телефон его владельца.

Без проблем взломать «умный дом» можно и находясь прямо на месте. Как правило, при создании таких систем, особенно для жилых помещений, к существующей инфраструктуре просто «пристраивается» дополнительный уровень новых устройств. Новые гаджеты общаются между собой с помощью протоколов для беспроводного взаимодействия. И часто разработчики систем выбирают протоколы, которые не предполагают шифрования, так что перехватить данные может любой человек, подключившийся к сети помещения.

Цель проекта: разработать систему обеспечения безопасности умного дома.

Задачи проекта:

- изучить проекты создания умных домов. Как работает система «умный дом»?
- ответить на вопросы «Что не так с “умным домом”?», «От чего следует защищать “умный дом”?»;
- определить слабое звено системы «умный дом»;
- как сделать «умный дом» безопаснее?
- представить проект архитектуры аппаратно-программного модуля, обеспечивающего безопасность «умного дома».

Ожидаемый результат:

Приобретение необходимых умений и навыков обеспечения безопасного функционирования умного дома.

План действий по реализации проекта

1. Организация работы в группах.
2. Обсуждение результатов.
3. Презентация результатов.

11 класс

ГЛАВА 2
СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

11 класс (35 часов)

Тема 1. Информация и информационные отношения. Субъекты информационных отношений, их интересы и сохранность, пути нанесения им вреда. Информационная безопасность (10 часов)

Материал для ознакомления

Технологии обеспечения информационной безопасности, защиты информации являются технологиями двойного назначения. Защита информации обладает существенным отличием от других технических направлений науки: защищенность информационной системы невозможно доказать или опровергнуть путем проверки этой системы на функционирование. При обосновании безопасности системы требуется думать за нарушителя, который предположительно владеет тем же специфичным набором средств, что и защитник. Поэтому знания в области создания защищенных информационных систем неотделимы от работ по построению новых вариантов атак. Данное обстоятельство определяет отбор содержания и глубину изучаемого учебного материала.

Факультативные занятия посвящены знакомству с правовыми нормами информационной деятельности человека. Существуют особенности информационной деятельности человека и проблемы, возникающие при взаимодействии общества и человека при рассмотрении информационного продукта как объекта собственности.

В современном обществе большинство людей занято деятельностью в информационной сфере, то есть сфере деятельности, связанной с созданием, преобразованием и потреблением информации. В основе производства, распространения, преобразования и потребления информации лежат информационные процессы сбора, создания, обработки, накопления, хранения, поиска информации в обществе, а также процессы создания и применения информационных систем и технологий.

При выполнении рассмотренных информационных процессов возникают социальные (общественные) отношения, которые подлежат правовому регулированию. Соответственно объектом правовых взаимоотношений выступает информация.

Существует юридически точное определение понятий, связанных с авторством и распространением компьютерных программ и баз данных. Определено, что авторское право распространяется на указанные объекты, являющиеся результатом творческой деятельности автора. Автор (или авторы) имеет исключительное право на выпуск в свет программ и баз данных, их распространение, модификацию и иное использование. Однако имущественные права на указанные объекты,

созданные в порядке выполнения служебных обязанностей или по заданию работодателя, принадлежат работодателю. Имущественные права, в отличие от авторских, могут быть переданы иному физическому или юридическому лицу на договорной основе.

Законодательство регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу и производство информации; применении информационных технологий; обеспечении защиты информации. В частности, утверждается право гражданина на получение из официальных источников информации о деятельности государственных органов, об использовании бюджетных средств, о состоянии окружающей среды и прочее, а также любой информации, непосредственно затрагивающей его права и свободы.

При этом обязанностью государства является создание условий для эффективного использования информационно-телекоммуникационных сетей, в том числе Интернета.

Действует закон «О персональных данных», целью которого является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных (с использованием средств автоматизации или без использования таких), в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Законодательно определена мера наказания за некоторые виды преступлений:

- неправомерный доступ к охраняемой законом компьютерной информации, если это повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации;
- создание, распространение или использование вредоносных программ;
- нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование информации.

По мере продвижения к информационному обществу все более острой становится проблема защиты права личности, общества и государства на конфиденциальность определенных видов информации. Другими словами, все более острой становится проблема информационной безопасности: защищенности информации и поддерживающей инфраструктуры информационной системы от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб субъектам информационных отношений (владельцам и пользователям информации) в рамках данной информационной системы.

Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная или, например, физическая). Основная задача информационной безопасности — сбалансированная защита конфиденциальности, целостности и доступности данных.

Защита информации — деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Различают несанкционированное и непреднамеренное воздействие на информацию.

Несанкционированным является воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации. Такого рода воздействие на информацию или ресурсы информационной системы может осуществляться с помощью вредоносных программ (вирусов).

Компьютерный вирус — это вредоносная программа, способная самопроизвольно присоединяться к другим программам и при запуске последних выполнять различные нежелательные действия: порчу файлов и каталогов; искажение результатов вычислений; засорение или стирание памяти; создание помех в работе компьютера. Наличие вирусов проявляется в разных ситуациях. Некоторые программы перестают работать или начинают работать некорректно. На экран выводятся посторонние сообщения, сигналы и другие эффекты. Работа компьютера существенно замедляется. Структура некоторых файлов оказывается испорченной.

Для борьбы с вирусами существуют программы, которые можно разбить на основные группы: мониторы, детекторы, доктора, ревизоры и вакцины.

Программы-мониторы (программы-фильтры) располагаются резидентно в оперативной памяти компьютера, перехватывают и сообщают пользователю об обращениях операционной системы, которые используются вирусами для размножения и нанесения ущерба. Пользователь имеет возможность разрешить или запретить выполнение этих обращений. К преимуществу таких программ относится возможность обнаружения неизвестных вирусов. Использование программ-фильтров позволяет обнаруживать вирусы на ранней стадии заражения компьютера. Недостатками программ являются невозможность отслеживания вирусов, обращающихся непосредственно к BIOS, а также загрузочных вирусов, активизирующихся до запуска антивируса при загрузке DOS, и частая выдача запросов на выполнение операций.

Программы-детекторы проверяют, имеется ли в файлах и на дисках специфическая для данного вируса комбинация байтов. При ее обнаружении выводится соответствующее сообщение. Недостаток — возможность защиты только от известных вирусов.

Программы-доктора восстанавливают зараженные программы путем удаления из них тела вируса. Обычно эти программы рассчитаны на конкретные типы вирусов и основаны на сравнении последовательности кодов, содержащихся в теле вируса, с кодами проверяемых программ. Программы-доктора необходимо периодически обновлять с целью получения новых версий, обнаруживающих новые виды вирусов.

Программы-ревизоры анализируют изменения состояния файлов и системных областей диска. Проверяют состояние загрузочного сектора и таблицы FAT; длину, атрибуты и время создания файлов; контрольную сумму кодов. Пользователю сообщается о выявлении несоответствия.

Программы-вакцины модифицируют программы и риски так, что это не отражается на работе программ, но вирус, от которого производится вакцинация, считает программы или диски уже зараженными.

Существующие антивирусные программы в основном относятся к классу гибридных (детекторы-доктора, доктора-ревизоры и прочее).

Информация так же может быть утеряна, искажена или блокирована непреднамеренно, например, из-за ошибочного действия пользователя или сбоя оборудования. Для предотвращения этого создаются резервные копии программ и документов. А большинство современных средств информационных технологий предусматривают автоматическое сохранение информационного продукта в ходе его разработки.

Защита от случайной потери или изменения информации осуществляется в основном следующими материалами:

- обязательным запросом на подтверждение команды, приводящей к изменению содержания какого-либо файла или группы файлов;
- установкой атрибутов, ограничивающий возможность изменения файла (например, с помощью атрибута «только для чтения»);
- возможностью отменить последнее действие;
- разграничением доступа пользователей к ресурсам, в частности с помощью системы паролей.

В ходе факультативных занятий «Информационная безопасность: миф или реальность?» вам необходимо выполнить практические задания, отражающие реальные ситуации по обеспечению информационной безопасности в контексте нормативно-правовых требований, законодательной базы (девиз: «Внимание: персональные данные!»), по решению проблем информационной и кибербезопасности с использованием специальных аппаратно-программных средств (девиз: «Интернет известный и неизвестный»), отражающих реальные ситуации поведения в сети и виртуальном общении (девиз «Сетевой этикет»), а также проблему информационно-психологической безопасности, активизирующих стремление к применению полученных компетенций в реальной жизни (девиз: «Подводные камни Интернета»).

В процессе факультативных занятий необходимо решить практические ситуационные задачи в контексте следующих понятий:

- главные понятия в области сохранности информации. Основные причины обострения проблемы обеспечения информационной безопасности;
- информационная безопасность. Угрозы безопасности информации в автоматизированных системах;
- объекты защиты. Виды мер противодействия угрозам безопасности;
- правовые базы обеспечения сохранности информации. Ответственность за нарушения в сфере защиты информации;
- идентификация и проверка подлинности пользователей;
- политика безопасности при доступе к общей сети;
- антивирусные средства защиты. Технологии обнаружения вирусов. Антивирусная защита как средство нейтрализации угроз.

Решение практических ситуационных задач:

- использование программных средств для тестирования и очистки операционной системы от вирусов и вредоносного программного обеспечения.
- использование средств администрирования операционной системы для настройки прав пользователей по доступу к информационным ресурсам;
- настройка средств системного межсетевого экрана (брандмауэра). Учетные записи пользователей. Конфигурирование простых маршрутизаторов. Резервное копирование ОС и данных пользователей.

Задание 1. Защита файлов от несанкционированного доступа с помощью архиваторов и средств Microsoft Office

Материал для ознакомления

В Word, Excel, Power Point и других программах MS Office есть возможность защиты файлов от несанкционированных изменений. Например, в Word существуют следующие возможности ограничения доступа к документу для защиты его от несанкционированных изменений:

- назначение пароля для открытия документа. Чтобы предотвратить любое открытие документа посторонними пользователями, можно назначить пароль;
- назначение пароля разрешения записи. Чтобы разрешить открытие документа всем пользователям, а изменение лишь некоторым, можно назначить пароль разрешения записи. Если какой-либо пользователь изменит документ без разрешения записи, он сможет сохранить этот документ только под другим именем;
- рекомендация доступа только для чтения. Можно предлагать (но не требовать) другим пользователям открыть документ только для чтения. Если пользователь откроет документ только для чтения и изменит его, он сможет сохранить этот документ только под другим именем.

В других программах MS Office также есть встроенные в эти программы средства защиты файлов от несанкционированных изменений, мы не будем их перечислять (более подробно познакомиться с ними можно с помощью справочной системы программ).

Однако следует помнить, что защита файлов встроенными средствами программ MS Office, позволяет защитить данные лишь от любопытства непрофессионалов. Об этом говорит существование программ подбора паролей к программам MS Office на тот случай, если пользователь забыл пароль. Выполняя задания, вы убедитесь в том, что «закрытый» паролем документ «открывается» одной из программ Passware Kit.

Самостоятельная работа

Изучите программы MS Office (Word, Excel, Access и др.). Они имеют встроенные средства защиты создаваемых файлов, которые позволяют при сохранении файлов указать пароль для открытия файла и пароль разрешения записи.

Изучите методы защиты файлов с помощью архиватора WinRAR.

Программы-архиваторы (WinZIP, WinRar) позволяют использовать криптографическую защиту, то есть выполнять операции архивирования и разархивирования файлов с паролем. Использование операции архивирования файла с паролем несколько надежнее, чем защита файлов встроенными средствами MS Office.

Задание 2. Защита папок и файлов. Поставить пароль на документ Word. Защита текстовых документов в Microsoft Word.

Материал для ознакомления

Как надежно скрыть папку или файл от посторонних глаз? Поставить пароль на документ Word необходимо по разным причинам: документ содержит секретные данные, конфиденциальную или приватную информацию.

В Сети существует много программ для скрытия отдельных папок и файлов от других пользователей компьютера. Эти программы предлагают простой

метод скрытия папок с помощью фильтрации запросов к файловой системе. Но это не означает 100 % защиту данных.

На самом деле скрытые файлы и папки можно увидеть и посмотреть с помощью других средств. Если требуется более надежная защита, следует обратиться к серьезным криптографическим пакетам (шифрование).

Для сохранности в тайне или в неприкосновенности таких записей, существует самый простой способ для решения проблемы приватности данных.

Для этого необходимо поставить пароль на документ Word. После установки пароля на документ Word, документ будет зашифрован. При открытии такого документа потребуется выполнить операции по вводу пароля.

Пароль желательно использовать сложный, для большей надежности. Простые пароли могут быть быстро расшифрованы специализированными программами для расшифровки паролей. Для создания надежного пароля будет лучше использовать специальную программу — менеджер паролей. С помощью такой программы можно создать пароль, а потом ввести его из менеджера паролей в окно поле ввода пароля в программе Word.

Практическая работа

Осуществите установку защиты на табличную форму представления информации:

Создайте бланк зарплатной ведомости организации (любой другой бланк учета информации), содержащий три (и более) раздела:

- Раздел 1 — «шапка» ведомости;
- Раздел 2 — таблица;
- Раздел 3 — дата создания ведомости, фамилии руководителя организации и главного бухгалтера. Установите защиту документа от изменений так, чтобы изменения можно было вносить только в поля форм и в таблицу с фамилиями и другими данными сотрудников организации. Также установить пароль на открытие файла.

Задание 3. Изучите возможности электронной таблицы MS Excel. Организуйте защиту файлов средствами электронной таблицы MS Excel.

Создайте таблицу MS Excel различного наполнения, индивидуальную для каждого учащегося.

Организуйте защиту содержимого таблицы, используя возможности MS Excel.

Задание 4. Изучите способы создания резервных копий базы данных. Создайте резервные копии файлов (для баз данных и проектов Access).

Создайте базу данных, индивидуальную для каждого учащегося. Обеспечьте ее защиту.

Задание 5. (Выполняется индивидуально или в малых группах.)
Создайте сайт и обеспечьте его защиту:

«Информационно-образовательная среда моей школы».
«Исторический сайт “Моя Беларусь”».
«Электронная библиотека с контролируемым доступом».
«Семейный сайт: история моей семьи».
«Супермаркет с электронным доступом и электронным заказом».
«Электронный кинотеатр».
«Любая другая среда по выбору».

Тема 2. Индивидуальные проекты в сфере информационной безопасности (10 часов)

Примерная тематика проектов: «Очистка операционной системы от вирусов и вредоносного программного обеспечения», «Обеспечение безопасности информационных систем и сетей», «Создание виртуальных частных сетей».

Проект «Очистка операционной системы от вирусов и вредоносного программного обеспечения»

Материал для ознакомления

Вирус — враг компьютера. Как и обычные вирусы, вирусы компьютерные — паразиты, для размножения им нужен «носитель», хозяин, здоровая программа или документ, в тело которой они прячут участки своего программного кода. Вирусы, получившие широкое распространение в компьютерной технике, взбудоражили весь мир. Многие пользователи компьютеров обеспокоены тем, что с помощью компьютерных вирусов злоумышленники взламывают сети, грабят банки, крадут интеллектуальную собственность...

Сегодня массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

Свойства компьютерных вирусов

Сейчас применяются персональные компьютеры, в которых пользователь имеет свободный доступ ко всем ресурсам машины. Именно это открыло возможность для опасности, которая получила название компьютерного вируса.

Что такое компьютерный вирус? Прежде всего, вирус — это вредоносная программа. В тот момент, когда мы, ничего не подозревая, запускаем на своем компьютере зараженную программу или открываем документ, вирус активизируется и заставляет следовать не нашим, а его инструкциям.

Вирус — программа, обладающая способностью к самовоспроизведению. Такая способность является единственным средством, присущим всем типам вирусов.

Вирус не может существовать в полной изоляции: сегодня нельзя представить себе вирус, который не использует код других программ, информацию о файловой структуре или даже просто имена других программ. Причина понятна: вирус должен каким-нибудь способом обеспечить передачу себе управления.

Классификация вредоносных программ (компьютерных вирусов)

В зависимости от среды обитания вирусы можно разделить на сетевые, файловые, загрузочные и файлово-загрузочные.

Сетевые вирусы распространяются по различным компьютерным сетям.

Файловые вирусы внедряются главным образом в исполняемые модули, то есть в файлы, имеющие расширения COM и EXE.

Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управления и, следовательно, теряют способность к размножению.

Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Re-cord).

Файлово-загрузочные вирусы заражают как файлы, так и загрузочные сектора дисков.

- По способу заражения вирусы делятся на резидентные и нерезидентные. *Резидентный вирус* при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.

  Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.
- По степени воздействия вирусы можно разделить на следующие виды:
  - *неопасные*, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках. Действия таких вирусов проявляются в каких-либо графических или звуковых эффектах.
  - *опасные* вирусы, которые могут привести к различным нарушениям в работе компьютера.
  - *очень опасные*, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.
- По особенностям алгоритма вирусы трудно классифицировать из-за большого разнообразия.

Простейшие вирусы — паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены.

Можно отметить вирусы-репликаторы, называемые червями, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии, распространяются по глобальным сетям, поражая целые системы, а не отдельные программы.

Известны вирусы-невидимки, называемые стелс-вирусами, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска. Стелс-вирусы обманывают антивирусные программы и в результате остаются незамеченными.

Наиболее трудно обнаружить вирусы-мутанты, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов.

Имеются и так называемые квазивирусные или «троянские» программы, которые хотя и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

Троянский конь — это программа, содержащая в себе некоторую разрушающую функцию, которая активизируется при наступлении некоторого условия срабатывания. Обычно такие программы маскируются под какие-нибудь полезные утилиты. Вирусы могут нести в себе троянских коней или «троянизировать» другие программы: вносить в них разрушающие функции.

Троянские кони представляют собой программы, реализующие помимо функций, описанных в документации, и некоторые другие функции, связанные с нарушением безопасности и деструктивными действиями. Отмечены случаи создания таких программ с целью облегчения распространения вирусов.

Программные закладки также содержат некоторую функцию, наносящую ущерб, но эта функция, наоборот, старается быть как можно незаметнее, так как чем дольше программа не будет вызывать подозрений, тем дольше закладка сможет работать.

Если вирусы и троянские кони наносят ущерб посредством лавинообразного саморазмножения или явного разрушения, то основная функция вирусов типа «червь», действующих в информационных сетях, — взлом атакуемой системы, т. е. преодоление защиты с целью нарушения безопасности и целостности.

Пути проникновения вирусов в компьютер

Основными путями проникновения вирусов в компьютер являются съемные носители информации, а также компьютерные сети. Заражение жесткого диска вирусами может произойти при загрузке программы с носителя, содержащего вирус.

Вирус, как правило, внедряется в рабочую программу таким образом, чтобы при ее запуске управление сначала передалось ему и только после выполнения всех его команд снова вернулось к рабочей программе. Получив доступ к управлению, вирус, прежде всего, переписывает сам себя в другую рабочую программу и заражает ее. После запуска программы, содержащей вирус, становится возможным заражение других файлов.

Наиболее часто вирусом заражаются загрузочный сектор диска и исполняемые файлы, имеющие расширения EXE, COM, SYS, BAT. Крайне редко заражаются текстовые файлы.

После заражения программы вирус может выполнить какую-нибудь диверсию, не слишком серьезную, чтобы не привлечь внимания. И, наконец, не забывает возвратить управление той программе, из которой был запущен. Каждое выполнение зараженной программы переносит вирус в следующую. Таким образом заразится все программное обеспечение.

Признаки появления вирусов

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести следующие:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе компьютера.

Методы защиты от вредоносных программ (компьютерных вирусов)

Каким бы ни был вирус, пользователю необходимо знать основные методы защиты от вредоносных программ.

Для защиты от вирусов можно использовать:

- общие средства защиты информации;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- специализированные программы для защиты от вирусов.

Имеются две основные разновидности общих средств защиты информации, которые полезны не только для защиты от вирусов:

- копирование информации — создание копий файлов и системных областей дисков;
- разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их недостаточно. Необходимо и применение специализированных программ для защиты от вирусов. Эти программы можно разделить на несколько видов: детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины.

Программы-детекторы, позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение. Многие детекторы имеют режимы лечения или уничтожения зараженных файлов.

Программы-ревизоры имеют две стадии работы. Сначала они запоминают сведения о состоянии программ и системных областей дисков (загрузочного сектора и сектора с таблицей разбиения жесткого диска). Предполагается, что в этот момент программы и системные области дисков не заражены. После этого с помощью программы-ревизора можно в любой момент сравнить состояние программ и системных областей дисков с исходным. О выявленных несоответствиях сообщается пользователю.

Существуют также программы-фильтры, которые располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.

Некоторые программы-фильтры не ловят подозрительные действия, а проверяют вызываемые на выполнение программы на наличие вирусов. Это вызывает замедление работы компьютера.

Программы-вакцины или иммунизаторы модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы крайне неэффективны.

Антивирусные программы

Антивирус едва ли не первая программа, которую следует установить на компьютер сразу после покупки, не следует даже пытаться выходить без него в Интернет.

На 100 % защититься от вирусов практически невозможно. Если же не вносить информацию в компьютер извне, заразиться вирусом невозможно, сам он не родится. Практически все существующие антивирусные программы просты и удобны в пользовании, способны отлавливать почти все существующие сегодня группы вирусов.

Большинство антивирусов способны не просто проверять по запросу пользователя диск на наличие вирусов, но и вести незаметную проверку всех запускаемых на компьютере файлов. Наконец, все современные антивирусы снабжены механизмом автоматического обновления антивирусных баз данных через Интернет.

План работы над проектом

1. Реализация проекта.
2. Презентация проекта.
3. Анализ работы над проектом.

Содержательная часть проекта должна включать следующие вопросы:

Введение.

1. История, понятие и классификация компьютерных вирусов.
   1.1. История создания компьютерных вирусов.
   1.2. Понятие и свойство компьютерных вирусов.
2. Компьютерные вирусы: классификация и виды.
   2.1. Классификация вирусов.
   2.2. Особые типы компьютерных вирусов.
3. Пути проникновения компьютерных вирусов в компьютер и способы защиты от них.
   3.1. Пути проникновения компьютерных вирусов в компьютер.
   3.2. Признаки появления компьютерных вирусов и основные эффекты, используемые вирусами.
   3.3. Методы защиты от компьютерных вирусов.
4. Практический пример реализации проекта.

Заключение.

Содержательная часть проекта носит рекомендательный характер. Проект может выполняться индивидуально или в микрогруппе.

Дополнительные темы проектов:

- «Компьютерные вирусы и антивирусная профилактика».

«Антивирусная защита. Технология тестирования компьютера».

«Профилактика заражения компьютера вирусами».

«Применение антивирусных средств защиты. Методы и средства защиты информации от несанкционированного доступа».

Проект «Обеспечение безопасности информационных систем и сетей»

Материал для ознакомления

В вычислительных сетях сосредоточивается информация, исключительное право на пользование которой принадлежит определенным лицам или группам лиц, действующим в личном порядке или в соответствии с должностными обязанностями. Такая информация должна быть защищена от всех видов постороннего вмешательства: чтения лицами, не имеющими права доступа к информации, и преднамеренного изменения информации.

Физическая защита системы и данных может осуществляться только в отношении рабочих ПК и узлов связи, но оказывается невозможной для средств передачи, имеющих большую протяженность. По этой причине в вычислительных сетях должны использоваться средства, исключающие несанкционированный доступ к данным и обеспечивающие их секретность.

Исследования практики функционирования систем обработки данных и вычислительных систем показали, что существует достаточно много возможных направлений утечки информации и путей несанкционированного доступа в системах и сетях. В их числе:

- чтение остаточной информации в памяти системы после выполнения санкционированных запросов;
- копирование носителей информации и файлов информации с преодолением мер защиты;
- маскировка под зарегистрированного пользователя;
- маскировка под запрос системы;
- использование программных ловушек;
- использование недостатков операционной системы;
- незаконное подключение к аппаратуре и линиям связи;
- злоумышленный вывод из строя механизмов защиты;
- внедрение и использование компьютерных вирусов.

Обеспечение безопасности информации в вычислительных сетях и в автономно работающих компьютерах достигается комплексом организационных, организационно-технических и программных мер.

✓ К организационным мерам защиты относятся:

- ограничение доступа в помещения, в которых происходит подготовка и обработка информации;
- допуск к обработке и передаче конфиденциальной информации только проверенных должностных лиц;
- хранение магнитных носителей и регистрационных журналов в сейфах, закрытых для доступа посторонних лиц;
- исключение просмотра посторонними лицами содержания обрабатываемых материалов через дисплей, принтер и другие устройства;
- использование криптографических кодов при передаче по каналам связи ценной информации;
- уничтожение красящих лент, бумаги и иных материалов, содержащих фрагменты ценной информации.

✓ Организационно-технические меры включают:

- осуществление питания оборудования, обрабатывающего ценную информацию от независимого источника питания или через специальные сетевые фильтры;
- установку на дверях помещений кодовых замков;
- уничтожение информации при списании или ремонте компьютера;
- ограничение электромагнитного излучения путем экранирования помещений, где проходит обработка информации, листами из металла или из специальной пластмассы.

✓ Технические средства защиты — это системы охраны территорий и помещений с помощью экранирования машинных залов и организации контрольно-пропускных систем.

Защита информации в сетях и вычислительных средствах с помощью технических средств реализуется на основе организации доступа к памяти с помощью:

- контроля доступа к различным уровням памяти компьютеров; блокировки данных и ввода ключей;
- выделения контрольных битов для записей с целью идентификации и другие способы.

✓ Архитектура программных средств защиты информации включает:

- контроль безопасности, в том числе контроль регистрации вхождения в систему;
- фиксацию в системном журнале, контроль действий пользователя;
- реакцию (в том числе звуковую) на нарушение системы защиты контроля доступа к ресурсам сети Интернет;
- контроль мандатов доступа;
- формальный контроль защищенности операционных систем (базовой, общесистемной и сетевой);
- контроль алгоритмов защиты;
- проверку и подтверждение правильности функционирования технического и программного обеспечения.

Для надежной защиты информации и выявления случаев неправомочных действий проводится регистрация работы системы: создаются специальные дневники и протоколы, в которых фиксируются все действия, имеющие отношение к защите информации в системе.

Фиксируются время поступления заявки, ее тип, имя пользователя и терминала, с которого инициализируется заявка.

Используются также специальные программы для тестирования системы защиты. Периодически или в случайно выбранные моменты времени они проверяют работоспособность аппаратных и программных средств защиты.

К отдельной группе мер по обеспечению сохранности информации и выявлению несанкционированных запросов относятся программы обнаружения нарушений в режиме реального времени. Программы данной группы формируют специальный сигнал при регистрации действий, которые могут привести к неправомерным действиям по отношению к защищаемой информации. Сигнал может содержать информацию о характере нарушения, месте его возникновения и другие характеристики. Кроме того, программы могут запретить доступ к защищаемой информации или симулировать такой режим работы (например, моментальная загрузка устройств ввода-вывода), который позволит выявить нарушителя и задержать его соответствующей службой.

Один из распространенных способов защиты — явное указание секретности выводимой информации. В системах, поддерживающих несколько уровней секретности, вывод на экран терминала или печатающего устройства любой единицы информации (например, файла, записи или таблицы) сопровождается специальным грифом с указанием уровня секретности.

Это требование реализуется с помощью соответствующих программных средств.

В отдельную группу выделены средства защиты от несанкционированного использования программного обеспечения.

В рамках общей темы следует выполнить следующие мини-проекты:
«Защита информации от несанкционированного доступа».
«Угрозы и уязвимости проводных корпоративных сетей».
«Модели безопасности по разграничению доступа в систему».
«Модели защиты при отказе в обслуживании».
«Модели безопасности по разграничению доступа в систему».
«Модель безопасности объектов вычислительных сетей».
«Построение системы антивирусной защиты корпоративной сети».

Проект «Создание виртуальных частных сетей»

План работы над проектом

1. Реализация проекта: «Построение VPN на базе специального программного обеспечения» (по выбору учителя совместно с учащимися).
2. Презентация проекта.
3. Анализ работы над проектом.

Содержательная часть проекта должна включать следующие вопросы:

1. Цель работы: ознакомиться с принципами построения VPN на базе программного обеспечения. (Задание рассчитано на работу в паре.)

2. Теоретическое обоснование проекта.

В процессе выполнения проекта учащийся или группа учащихся совместно с учителем выбирают ту или иную технологию, позволяющую обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет).

Необходимо выбрать тот или иной метод реализации, на одном из которых базируется виртуальная частная сеть.

Специальное программное обеспечение позволяет создать виртуальную частную сеть (VPN) через Интернет и объединить в ней несколько компьютеров. После создания такой сети пользователи могут устанавливать VPN-сессии между собой и работать в этой сети точно так же, как в обычной локальной (LAN) сети с возможностью обмена файлами, удаленного администрирования компьютеров и т. д.

3. Создать локальную сеть (на основе изученных теоретических сведений, презентация, пункт 2).

4. Объединить в сеть принтер, камеру или другое устройство либо развернуть в сети какое-либо программное обеспечение (например, игру) (по выбору учащихся совместно с учителем).

5. Подготовить отчет.

Тема 3. Выполнение группового проекта (14 часов)

Выполнение группового проекта предполагает погружение в проблему: выбор темы, постановка цели и задач, поиск и анализ информации.

В процессе выполнения проекта организуется групповая деятельность по выполнению поставленных задач совместного проекта: обсуждение возможных вариантов решения поставленных задач, сравнение возможных стратегий, выбор оптимальной стратегии, совместное составление плана действий, распределение обязанностей.

Деятельность по выполнению проекта сопровождается выбором программного решения с внесением при необходимости изменений, совместное выполнение каждого этапа проекта с анализом полученных результатов.

Итогом группового проекта является презентация полученных результатов и защита проекта группой.

Этапы работы над проектом

1. Введение в проектную деятельность.
2. Определение и утверждение тематики проекта.
3. Составление графика работы над проектом.
4. Подбор и анализ источников.
5. Анализ и контроль процесса выполнения проекта (консультации).
6. Контроль за оформлением проекта.
7. Организация и проведение предзащиты проекта.
8. Контроль за доработкой проекта.
9. Защита проекта.
10. Подведение итогов работы.

Тематика проектов:

«Разработка защищенной корпоративной сети».

«Обеспечение защиты интеллектуальной собственности в Интернете».

«Береги пароль смолоду, а антивирус держи в свежести».

Проект «Разработка защищенной корпоративной сети»

Материал для ознакомления

Корпоративная вычислительная сеть — это сложный комплекс взаимосвязанных и согласованно функционирующих программных и аппаратных компонентов.

Изучение сети в целом предполагает знание принципов работы ее отдельных элементов:

- компьютеров;
- коммуникационного оборудования;
- операционных систем;
- сетевых приложений.

План работы над проектом

1. Реализация проекта.
2. Презентация проекта.
3. Анализ работы над проектом.

Содержательная часть проекта должна включать следующие вопросы:

Цель: разработать проект корпоративной сети.

Задачи:

- сравнить ряд существующих технологий;
- создать проект корпоративной информационной сети в соответствии с разработанным техническим заданием, используя полученные при сравнении технологий данные;
- реализовать проект (исходя из оснащенности аппаратно-программными средствами);
- наблюдая за полученной системой, сделать выводы.

Проект «Обеспечение защиты интеллектуальной собственности в Интернете»

Материал для ознакомления

Интеллектуальная собственность — в широком понимании термин означает закрепленное законом временное исключительное право, а также личные неимущественные права авторов на результат интеллектуальной деятельности или средства индивидуализации.

Цель проекта:

- изучить проблемы, связанные с защитой авторских и иных смежных прав в сети Интернет;
- исследовать пиратское распространение информации в Интернете;
- ознакомиться с понятиями «интеллектуальная собственность», «нарушение авторского права».

Задачи проекта:

- проанализировать, как можно защитить открытую информацию от ненадлежащего ее использования.

Проект должен состоять:

- из введения,
- основной части,
- заключения,
- списка использованных источников,
- приложений.

Проект «Береги пароль смолоду, а антивирус держи в свежести»

Материал для ознакомления

Одним из важнейших процессов, создаваемых для соблюдения такого свойства информации, как конфиденциальность, является ограничение доступа. Наиболее распространен такой процесс аутентификации как использование пароля. Практически с момента создания первых многопользовательских операционных систем для ограничения доступа используются пароли.

План работы над проектом

1. Реализация проекта.
2. Презентация проекта.
3. Анализ работы над проектом.

Содержательная часть проекта должна включать следующие вопросы:

Цель проекта: рассмотреть использование паролей как средства решения проблемы кибербезопасности; рассмотреть возможные способы применения современных методов и средств защиты информационных ресурсов.

Задачи:

- изучить и проанализировать тему кибербезопасности;
- выявить проблемы кибербезопасности, изучить типы угроз, элементы кибербезопасности;
- проанализировать способы решения этих проблем;
- научиться использовать безопасные пароли;
- создать фильм-инструкцию о формировании паролей.