Межрегиональный телекоммуникационный проект
для педагогов, специалистов и руководителей образовательных учреждений
"Методическая поддержка обеспечения информационной безопасности детей"
(Координатор проекта - ГАОУДПО ВИПКРО имени Л.И. Новиковой)

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по обеспечению
информационной безопасности обучающихся
системы профессионального образования

Авторы-составители:

Ерофеева Анастасия Олеговна, *ассистент кафедры физики и информационных технологий, Балашовский институт (филиал) ФГБОУ ВПО "Саратовский государственный университет имени Н.Г. Чернышевского" г. Балашов;*

Кульков Александр Александрович, заместитель директора по УПР ГБОУ СПО ВО “Ковровский промышленно-гуманитарный техникум” г. Ковров;

Мурылева Галина Александровна, преподаватель информатики и ИКТ ГБОУ НПО Владимирской области “Профессиональное училище № 10” г. Муром;

Никишина Татьяна Павловна, преподаватель физики и информатики ГБОУ СПО ВО “Муромский промышленно-гуманитарный техникум г. Муром;

Тимина Наталья Владимировна, социальный педагог, преподаватель психологии и педагогики, ГБОУ СПО ВО “Муромский педагогический колледж” , г. Муром;

Топоркова Наталия Ивановна, методист МАОУ ДПО ИПК г. Новокузнецк.

2013 год

Аннотация

В настоящей работе рассматриваются различные аспекты понятия “информационная безопасность” в системе начального, среднего и высшего профессионального образования.

Методические рекомендации предназначены администрации, преподавателям и обучающимся системы профессионального образования для использования при организации и обеспечении информационной безопасности образовательных учреждений.

Некоторые разделы могут быть полезны родителям подростков, желающим оградить своих детей от различных опасностей, угроз, которые таят в себе “виртуальная реальность” Интернета, компьютерные игры, а также неумелое использование компьютера и мобильной связи.

Данные методические рекомендации разработаны в рамках Межрегионального телекоммуникационного проекта для педагогов, специалистов и руководителей образовательных учреждений “Методическая поддержка обеспечения информационной безопасности детей” на основе профессионального опыта авторов-разработчиков, а также их коллег из различных субъектов Российской Федерации.

ОГЛАВЛЕНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Информационная безопасность в системе профессионального образования — составное понятие, включающее технические, этические и правовые аспекты.

В настоящее время каждый из обучающихся в системе профессионального образования использует компьютер и доступ в Интернет, причем большинство учащихся имеет эти инструменты получения информации дома. Поскольку глобальная сеть Интернет наряду с уникальными возможностями для системы образования таит в себе и чрезвычайную опасность, преподаватели и студенты, все активнее использующие средства новых информационных технологий, ресурсы и услуги Интернет, должны не только осознавать, какой вред может быть нанесен их интеллектуальному, нравственному развитию, психическому и физическому здоровью, но знать и уметь пользоваться средствами защиты от нее. Эта опасность, разумеется, кроется во всех средствах массовой информации, и в первую очередь, в ТВ, радио, печатных изданиях.

Преподавание информационной безопасности в профессиональном образовании развивается в двух направлениях:

- собственно компьютерная безопасность – развитие у студентов навыков культурного поведения в сети, использования лицензированных продуктов, познаний в области антивирусного и антиспамового программного обеспечения.
- медиаобразование, т. е. изучение специфического языка различных средств массовой информации: телевидения, радио, прессы, Интернета, чтобы уметь правильно и критически работать с информацией.

Особое значение в этом направлении приобретает интеллектуальное развитие студентов в рамках профессионального образования, так как после его завершения студенты переходят непосредственно к трудовой деятельности, и зачастую не имеют достаточно времени для получения новых, дополнительных знаний.

В этой связи важное значение в системе профессионального образования придается методическим рекомендациям по обеспечению информационной безопасности обучающихся системы профессионального образования, которые предназначены для оказания помощи администрации, преподавателям и обучающимся в организации и обеспечении информационной безопасности образовательных учреждений. Кроме того, предлагаемые материалы могут служить основой для проведения занятий по различным дисциплинам.

Особенностью настоящей работы является подробное рассмотрение практики обеспечения информационной безопасности обучающихся системы профессионального образования, а также обобщение материалов по данной теме, учитывающих интересы как педагогов, так и родителей учащихся.

Основные термины и понятия

Áвторское прáво — институт гражданского права, регулирующий отношения, связанные с созданием и использованием произведений науки, литературы или искусства. Программы для ЭВМ и базы данных также охраняются авторским правом.

Аккаунт, или учетная запись - запись, содержащая сведения, которые пользователь сообщает о себе некоторой компьютерной системе.

Активная угроза - преднамеренное несанкционированное изменение состояния системы.

Антивирусная программа (антивирус) — программа, предназначенная для обнаружения компьютерных вирусов, а также вредоносных программ и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Атака - нарушение безопасности информационной системы, позволяющее захватчику управлять операционной средой. DoS-атака (атака типа «отказ в обслуживании») — атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легальные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам (серверам), либо этот доступ затруднён.

Баннер - графическое изображение рекламного характера, аналогичное рекламному модулю в прессе. Может быть как статичным изображением или даже текстом, так и содержать анимированные элементы (вплоть до видео и интерактивных объектов).

Блог - веб-сайт, основное содержимое которого — регулярно добавляемые записи (посты), содержащие текст, изображения или мультимедиа. Отличия блога от традиционного дневника обусловливаются средой: блоги обычно публичны и предполагают сторонних читателей, которые могут вступить в публичную полемику с автором (в комментарии к блогозаписи или своих блогах). Под блогами также понимаются персональные сайты, которые состоят в основном из личных записей владельца блога и комментариев пользователей к этим записям. Людей, ведущих блог, называют блóггерами. Совокупность всех блогов Сети принято называть блогосферой.

Бэкдор, backdoor — программы, которые устанавливает взломщик на взломанном им компьютере после получения первоначального доступа с целью повторного получения доступа к системе.

Веб-обозревáтель, обозревáтель, брáузер - программное обеспечение для просмотра веб-сайтов, то есть для запроса веб-страниц (преимущественно из Сети), их обработки, вывода и перехода от одной страницы к другой.

Вишинг - назван так по аналогии с фишингом - распространённым сетевым мошенничеством. Сходство названий подчеркивает тот факт, что принципиальной разницы между вишингом и фишингом нет. Основное отличие вишинга в том, что так или иначе задействуется телефон (В случае вишинга в сообщении содержится просьба позвонить на определённый городской номер. При этом зачитывается сообщение, в котором потенциальную жертву просят сообщить свои конфиденциальные данные.

Например, ввести номер карты, пароли, PIN — коды, коды доступа или другую личную информацию в тоновом наборе)
Вредоносная программа, вредоносное ПО - любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного владельцем использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу ЭВМ, и/или владельцу сети ЭВМ, путем копирования, искажения, удаления или подмены информации.
Геймер - человек, играющий в видеоигры, хотя сначала геймерами называли тех, кто играет только в ролевые или военные игры. Несмотря на то, что термин включает в себя людей, не считающих себя полноправными игроками, ими часто называют тех, кто проводит много времени за играми или интересуется ими.
Гиперссылка - часть гипертекстового документа, ссылающаяся на другой элемент (команда, текст, заголовок, примечание, изображение) в самом документе, на другой объект (файл, каталог, приложение), расположенный на локальном диске или в компьютерной сети, либо на элементы этого объекта.
Доме́нное имя - символьное имя, служащее для идентификации областей — единиц административной автономии в сети Интернет — в составе вышестоящей по иерархии такой области. Каждая из таких областей называется доме́ном.
Загрузочный вирус — компьютерный вирус, записывающийся в первый сектор гибкого или жесткого диска и выполняющийся при загрузке компьютера.
Защи́та персона́льных да́нных — комплекс мероприятий технического, организационного и организационно-технического характера, направленных на защиту сведений, относящихся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).
Игровая зависимость, гейминг — форма психологической зависимости, проявляющаяся в навязчивом увлечении видеоиграми и компьютерными играми.
Интерне́т-зави́симость (или Интернет-адди́кция) — навязчивое желание подключиться к Интернету и болезненная неспособность вовремя отключиться от Интернета.
Интернет-цензура — контроль и пресечение публикации или доступа к информации в сети Интернета. Информационная безопасность — все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчётности, аутентичности и достоверности информации или средств её обработки.
Кейло́гер, кейло́ггер — это шпионское программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя - нажатия клавиш на клавиатуре компьютера, движения и нажатия клавиш мыши и т.д.
Кибермоббинг, Интернет-моббинг, кибербуллинг — это термин, под которым понимают намеренные оскорбления, угрозы, диффамации и сообщение другим компрометирующих данных с помощью современных средств коммуникации, как правило, в течение продолжительного периода времени.
Компью́терный ви́рус — разновидность компьютерных программ или вредоносный код, отличительным признаком которых является способность к размножению (саморепликация).
Ку́ки, cookie, cookies — небольшой фрагмент данных, отправленный веб-сервером и хранимый на компьютере пользователя. Веб-клиент (обычно веб-браузер) всякий раз при попытке открыть страницу соответствующего сайта пересылает этот фрагмент данных веб-серверу в виде HTTP-запроса. Применяется для сохранения данных на стороне пользователя, на практике обычно используется для:

- аутентификации пользователя;
- хранения персональных предпочтений и настроек пользователя;

- отслеживания состояния сессии доступа пользователя;
- ведения статистики о пользователях.

Логин — имя (идентификатор) учётной записи пользователя в компьютерной системе или процедура входа (идентификации и затем аутентификации) пользователя в компьютерную систему, как правило, путём указания имени учётной записи и пароля.
Макровирус — это разновидность компьютерных вирусов разработанных на макроязыках, встроенных в такие прикладные пакеты ПО, как Microsoft Office.
Межсетевой экран или сетевой экран, брандмауэр, файрво́лл, файрво́л, файерво́л, фаерво́л — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа.
Облачные вычисления, “облачные технологии”, в информатике — это модель обеспечения повсеместного и удобного сетевого доступа по требованию к общему пулу конфигурируемых вычислительных ресурсов (например, сетям передачи данных, серверам, устройствам хранения данных, приложениям и сервисам — как вместе, так и по отдельности), которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами и/или обращениями к провайдеру. Термин «облако» используется как метафора, основанная на изображении Интернета на диаграмме компьютерной сети, или как образ сложной инфраструктуры, за которой скрываются все технические детали.
Пароль — это секретное слово или набор символов, предназначенный для подтверждения личности или полномочий. Пароли часто используются для защиты информации от несанкционированного доступа.
Персональные данные - любая информация, относящаяся к определенному или определяемому физическому лицу (в том числе: его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, и т.д.)
Полиморфизм компьютерного вируса — специальная техника, используемая авторами вредоносного программного обеспечения для снижения уровня детектирования вредоносной программы классическими антивирусными продуктами.
Резервное копирование — процесс создания копии данных на носителе (жёстком диске, дискете и т.д.), предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения.
Руткит — программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе.
Сайт — совокупность электронных документов (файлов) частного лица или организации в компьютерной сети, объединённых под одним адресом (доменным именем или IP-адресом).
Се́рвер - 1. Программное обеспечение, принимающее запросы от клиентов; 2. Компьютер (или специальное компьютерное оборудование), выделенный и/или специализированный для выполнения определенных сервисных функций.
Сетевой этике́т, нетикет — правила поведения, общения в Сети традиции и культура интернет-сообщества, которых придерживается большинство.
Сигнату́ра ата́ки (вируса) — характерные признаки атаки или вируса, используемые для их обнаружения.
Социальная инженерия — это метод несанкционированного доступа к информации или системам хранения информации без использования технических средств. Основной целью социальных инженеров, как и других хакеров и взломщиков, является получение доступа к защищенным системам с целью кражи информации, паролей, данных о кредитных картах и т.п. Основным отличием от простого взлома является то, что в данном случае в

роли объекта атаки выбирается не машина, а ее оператор. Именно поэтому все методы и техники социальных инженеров основываются на использовании слабостей человеческого фактора, что считается крайне разрушительным, так как злоумышленник получает информацию, например, с помощью обычного телефонного разговора или путем проникновения в организацию под видом ее служащего.

Спам — рассылка коммерческой и иной рекламы или иных видов сообщений (информации) лицам, не выражавшим желания их получать. В общепринятом значении термин «спам» в русском языке впервые стал употребляться применительно к рассылке электронных писем.

Стелс-вирус (вирус-невидимка) — вирус, полностью или частично скрывающий свое присутствие в системе, путем перехвата обращений к операционной системе, осуществляющих чтение, запись, чтение дополнительной информации о зараженных объектах (загрузочных секторах, элементах файловой системы, памяти и т. д.)

Файловый вирус — компьютерный вирус, распространяющийся путем внедрения своего кода в тело исполняемых файлов.

Файлообменник, файлхостинг или файловый хостинг — сервис, предоставляющий пользователю место под его файлы и круглосуточный доступ к ним через web, как правило по протоколу http. Такой сервис позволяет удобно «обмениваться» файлами.

Фарминг — это процедура скрытного перенаправления жертвы на ложный IP-адрес.

Флуд — сообщения в интернет-форумах и чатах, занимающие большие объемы и/или не несущие никакой полезной информации. Технический флуд представляет собой хакерскую атаку с большим количеством запросов, приводящую к отказу в обслуживании.

Чат, чаттер — средство обмена сообщениями по компьютерной сети в режиме реального времени, а также
программное обеспечение, позволяющее организовывать такое общение.

Эксплойт, эксплоит, сплоит — компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости впрограммном обеспечении и применяемые для проведения атаки на вычислительную систему. Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение её функционирования (DoS-атака).

Электро́нная по́дпись (ЭП), Электро́нная цифровая по́дпись (ЭЦП) — информация в электронной форме, присоединенная к другой информации в электронной форме (электронный документ) или иным образом связанная с такой информацией. Используется для определения лица, подписавшего информацию (электронный документ).

Электро́нная по́чта, email, e-mail — технология и предоставляемые ею услуги по пересылке и получению электронных сообщений (называемых «письма» или «электронные письма») по распределённой (в том числе глобальной) компьютерной сети. Электронная почта по составу элементов и принципу работы практически повторяет систему обычной (бумажной) почты, заимствуя как термины (почта, письмо, конверт, вложение, ящик, доставка и другие), так и характерные особенности — простоту использования, задержки передачи сообщений, достаточную надёжность и в то же время отсутствие гарантии доставки.

Электронное сообщение — 1. Информация, переданная или полученная пользователем информационно-телекоммуникационной сети; 2. Файл, формируемый адресантом с помощью почтового клиента, предназначенный для передачи адресату посредством электронной почты.

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

ЖМД (HDD), он же винчестер, он же винт (винчестер, HDD - Hard Disk Drive) - предназначен для долговременного хранения всей имеющейся в компьютере информации. Информация хранится на одной или нескольких круглых пластинах с магнитным слоем, над поверхностью которых перемещаются магнитозаписывающие головки

ИБ - информационная безопасность

ИКТ - информационно-коммуникационные технологии, ИТ или IT - информационные технологии
ИС - информационная система
НСД - несанкционированный доступ
ПК - персональный компьютер
ПО - программное обеспечение
ТВ - телевидение
ЭВМ - электронно-вычислительная машина - комплекс технических средств, предназначенных для автоматической обработки информации в процессе решения вычислительных и информационных задач. Название «ЭВМ», принятое в русскоязычной научной литературе, является синонимом компьютера
ЭП, ЭЦП - Электронная (цифровая) подпись
DNS (англ. Domain Name System — система доменных имён) — компьютерная распределенная система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства)
FTP - протокол передачи файлов в компьютерных сетях
HTTP - англ. HyperText Transfer Protocol — протокол передачи гипертекста
IP-адрес - сетевой адрес узла в компьютерной сети, построенной по протоколу IP
IPS - система предотвращения вторжений (англ. Intrusion Prevention System) — программная или аппаратная система сетевой и компьютерной безопасности, обнаруживающая вторжения или нарушения безопасности и автоматически защищающая от них
SSL - это технология, обеспечивающая безопасное соединение между веб-сервером и программным обеспечением клиента (Safe Server Link)
UAC (англ.) - контроль учётных записей пользователей. UAC - это компонент операционных систем Microsoft Windows, впервые появившийся в Windows Vista, запрашивающий подтверждение действий, требующих прав администратора, в целях защиты от несанкционированного использования компьютера вредоносными программами, проще говоря - вирусами
URL - это адрес страницы в Интернете
VPN Virtual Private Network - виртуальная частная сеть. Защищенная сеть передачи данных, построенная на базе сети передачи данных общего пользования (интернет) с использованием туннелирующих протоколов и средств шифрования трафика

НОРМАТИВНО-ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ

Федеральный закон российской Федерации от № 63-ФЗ “Об электронной подписи” http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=132463
Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации"
Закон РФ "Об авторском праве и смежных правах"
Закон РФ “Об образовании” № 273-ФЗ http://www.eduhelp.info/page/federalnyj-zakon-ob-obrazovanii-v-rossijskoj-federacii-podpisal-putin
Федеральный закон от 10 января 2002 г. N 1-ФЗ “Об электронной цифровой подписи” Принят Государственной Думой 13 декабря 2001 года. Одобрен Советом Федерации 26 декабря 2001 года http://www.iiikt.narod.ru/osnov/mat12/law1fz.htm
Постановление от 26 октября 2012 г. N 1101

“О единой автоматизированной информационной системе "Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети “Интернет” и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети “Интернет” содержащие информацию, распространение которой в РФ запрещено" http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=137077;div=LAW;mb=LAW;opt=1;ts=06E4F8BCDF1B5C4FC3CD32E170A2B2D3
Уголовный кодекс (УК РФ) Раздел IX. Преступления против общественной безопасности и общественного порядка . Глава 28. Преступления в сфере компьютерной информации http://base.garant.ru/10108000/29/
Надзор в сфере информационных технологий http://www.rsoc.ru/treatments/p459/p463/
Закон о создании единого реестра доменов и сайтов с противоправным контентом, 11 июля 2012 г. http://www.dp.ru/a/2012/07/11/Gosduma_prinjala_zakon_o_ch/
Федеральный закон (проект) о внесении изменений в отдельные законодательные акты Российской Федерации по вопросам регулирования отношений при использовании информационно-телекоммуникационной сети Интернет. http://i-deti.org/upload/iblock/3de/lbi-110921133142-phpapp02.pdf
Федеральный закон “О защите детей от информации, причиняющей вред их здоровью и развитию” (в ред. Федерального закона от 28.07.2012 N 139-ФЗ) http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=133372;fld=134;dst=4294967295;rnd=0.39871055679395795;from=108808-0
Проект закона Лиги безопасного интернета «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам регулирования отношений при использовании информационно-телекоммуникационной сети Интернет» http://www.i-deti.org/legislation/
Д.П. Звоненко “Правила информационной безопасности детей” http://www.otraslychet.ru/article.php?page_date=0&page_number=0&rubr_type=rt_journal&rubr_id=1&page_id=9612
Указ Президента Российской Федерации от 1 июня 2012 года О национальной стратегии действий в интересах детей на 2012-2017 годы http://base.garant.ru/70183566/
Федеральный закон № 152-ФЗ «О персональных данных»
ВРЕМЕННЫЙ РЕГЛАМЕНТ исполнения государственной функции создания, формирования и ведения единой автоматизированной системы «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено». http://www.rspectr.com/index.php/к-обсуждению/item/203-единый-реестр-доменных-имен.html

(По материалам электронного научно-технического издания “Наука и образование” (http://techno-new.developer.stack.net/doc/143237.html)

Современный мир совершает переход из XX, «энергетического», века в XXI век, который со всей определенностью называют «информационным». Сегодня на смену индустриальному этапу общественного развития приходит информационный, при котором эффективное и динамичное развитие всех социально-экономических структур и общества в целом возможно только на основе максимально полного использования имеющихся информационных ресурсов.

Информация как предмет труда становится все в большей степени стратегическим ресурсом общества, его движущей производительной силой.

В условиях информатизации общества особую ценность приобретают люди - носители знаний, передатчики технологической информации и передового опыта. Создается мощнейшая инфраструктура средств компьютерной и телекоммуникационной техники, способная изменить не только процесс и характер трудовой деятельности, но и сам образ жизни, систему ценностей человека. Хорошо налаженная сеть информационно-вычислительных комплексов играет такую же роль в современном обществе, какую в свое время сыграли электрификация, телефонизация, радио и телевидение вместе взятые. Современные информационные технологии приобретают глобальный характер, охватывая все сферы жизнедеятельности человека, формируя информационное единство всей человеческой цивилизации. С помощью глобальной сети Интернет объединяются и перемещаются на любые расстояния гигантские объемы информации, обеспечивается доступ многочисленных пользователей, расположенных на практически неограниченной территории, к информационным ресурсам всего мирового сообщества.

В связи с тем, что информация превратилась из абстрактного понятия в едва ли не самый ценный объект во Вселенной, и ход всех значимых событий в науке, коммерции, социуме связан с процессами производства и владения информацией, возникла необходимость развития такой области информационных технологий (ИТ) как информационная безопасность (ИБ).

Впервые в России понятие «информационная безопасность» было введено в 1990 г. парламентской комиссией академика Ю.А. Рыжова, которая занималась разработкой концепции национальной безопасности страны. С тех пор созданы соответствующие структуры в Правительстве РФ, в Администрации Президента РФ, в Совете безопасности РФ, которые занимаются напрямую этими вопросами. В 1996 г. был создан парламентский подкомитет по информационной безопасности. Вопросы информационной безопасности заняли прочную строчку во всех посланиях Президента РФ, они вошли в Концепции по национальной безопасности, утвержденные 17 декабря 1997 г. и 10 января 2000 г.

Исходя из того, что информационная безопасность в начале третьего тысячелетия выходит на первое место в системе национальной безопасности, приоритетным становится формирование и проведение единой государственной политики в этой сфере. В современном мире, когда формируется и развивается информационное общество, когда разворачивается глобальная информационная война, известный афоризм «кто владеет информацией, тот владеет миром» является весьма актуальным. Кроме того, успех военных действий на суше, в воздухе и на море, в равной степени, как и предотвращение войны, военно-политических кризисов или вооруженных конфликтов существенно зависят от эффективности использования космической информации. Словосочетание «информационная безопасность» в разных контекстах может иметь различный смысл. В Доктрине информационной безопасности Российской Федерации информационная безопасность понимается в широком смысле как «состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства».

В более узком смысле под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.
Комплекс мероприятий, направленных на обеспечение ИБ, основан на системном подходе, определяющем субъекты, средства, объекты, источники опасности, направленность опасных информационных потоков и принципы обеспечения информационной безопасности.
Объектами опасного информационного воздействия и, следовательно, информационной безопасности считаются сознание, психика людей; информационно-технические системы различного масштаба и назначения.
К субъектам информационной безопасности относят те органы и структуры, которые занимаются ее обеспечением.
Средствами обеспечения информационной безопасности являются средства, с помощью которых осуществляются меры по защите информации, систем управления, связи, компьютерных сетей, недопущению подслушивания, маскировке, предотвращению хищения информации и т.д.

СОДЕРЖАНИЕ

Советы педагогам

(по материалам сайта “Безопасность в Интернете”)

Три основные правила безопасного Интернета

1) Защитите свой компьютер

- Регулярно обновляйте операционную систему.
- Используйте антивирусную программу.
- Применяйте брандмауэр.
- Создавайте резервные копии важных файлов.
- Будьте осторожны при загрузке содержимого.

2) Защитите себя в Интернете

- С осторожностью разглашайте личную информацию.
- Думайте о том, с кем разговариваете.
- Помните, что в Интернете не вся информация надежна и не все пользователи откровенны.

3) Соблюдайте правила

- Закону необходимо подчиняться даже в Интернете.
- При работе в Интернете не забывайте заботиться об остальных так же, как о себе.

Как рассказать учащимся об информационной безопасности (советы по проведению занятий)

Различные аспекты темы “Информационная безопасность” можно рассматривать на занятиях по следующим дисциплинам: информатика, информационные технологии, социология, безопасность жизнедеятельности, а также гражданское право.

Пример структуры занятия:

1. Мозговой штурм

– Что вы знаете об информационной безопасности? Что или кто может угрожать информации? Почему тема информационной безопасности является важной и почему эти вопросы должны обсуждаться в учебном заведении? (Из возможных причин можно

выделить аспекты, связанные с сущностью Интернета и его значимостью как средства общения).
2. Разбор различных ситуаций по теме занятия
– Учащимся можно предложить разобрать различные ситуации (например, в виде рассказов), связанные с темой занятия, посмотреть обучающие видеоролики или привести примеры из своей жизни (сталкивались ли они когда-нибудь с угрозами информации, вредоносными программами и т.д.).
3. Обсуждение
– После прочтения рассказов и/или просмотра видео разделите учащихся на группы для обсуждения затронутых проблем с помощью вопросов, приведенных в рассказах или видео.
– Очень важно включить в обсуждение личный опыт и мнения детей по вопросу информационной безопасности в Интернете.
Примерные темы для обсуждения:
Что включает в себя личная информация?
Имя и адрес — да; тем не менее, к личной информации также относятся другие сведения, которые могут быть связаны с человеком, например, номер мобильного телефона, адрес школы, место проживания и адрес электронной почты.
(В аудитории можно также изучить веб-сайт http://www.infosecurity.ee, который содержит более подробную информацию по вопросу информационной безопасности).
Интернет-угрозы, подстерегающие пользователей Интернета
1. Доступ к нежелательному содержимому:
- сайты и форумы, провоцирующие суициды;
- наркосайты;
- сайты, разжигающие национальную рознь и расовое неприятие: экстремизм, национализм, фашизм;
- сайты порнографической направленности;
- сайты знакомств;
- сайты различных религиозных сект.
2. Сообщение конфиденциальной информации собеседникам в сети (полное имя, адрес, номер интернет-кошелька, банковской карты родителей, места прогулок, время возвращения домой членов семьи и пр.)
3. Контакты с незнакомыми людьми посредством чатов, интернет-пейджеров, электронной почты и т.д. (среди них могут быть как мошенники, выпытывающие конфиденциальную информацию, так и педофилы), назначение личных встреч
4. Угроза заражения компьютера вредоносным ПО
5. Неконтролируемые покупки в интернет-магазинах и т.д.

Методические рекомендации к проведению мероприятия "3D-Безопасный Интернет" (или 3 Дня безопасного Интернета)

1 D - Первый день: массовое анкетирование учащихся, родителей и педагогов (может проводиться с использованием сервиса Google Формы) и изучение проблемы обеспечения информационной безопасности в учреждениях профессионального образования (образец анкет представлен в Приложениях 5-7, есть печатный вариант, а также онлайн-вариант в Google Формах - для доступа к ним просто щелкните мышкой на названии каждой анкеты).
2 D - Второй день: самый активный, в ходе которого проводятся конкурсы, викторины или другие мероприятия с применением интерактивных образовательных технологий (примерные вопросы для викторины представлены в Приложении 4). Можно организовать конференцию в формате World Cafe, или Мировое Кафе (это технология организации дискуссии в малых группах в непринужденной обстановке, подробнее о данной технологии можно узнать на сайте: http://www.theworldcafe.com или здесь!) и привлечь к участию в ней не только учащихся, но и педагогов и родителей. Один из вариантов

проблемных вопросов для дискуссии: Почему необходимо защищать информацию и как это можно сделать?
3 D - Третий день: день подведения итогов и изготовление буклета, флаера, глога или коллажа - "настольной книги" для детей и родителей (ссылки на образец буклета и коллажа для мероприятия указаны в разделе Приложения).

Рекомендации родителям - как обеспечить безопасность подростка в Интернете (по материалам информационного портала "Справочник Google по детской безопасности в Интернете" http://www.google.ru/goodtoknow/familysafety/")

История развития технологий не знает другого времени, когда бы дети и подростки столь же быстро, как сегодня, получали доступ к онлайн, конвергентным, мобильным и сетевым медиа. Обращение детей и подростков к Интернет-пространству включает многочисленные факторы, в совокупности формирующие модель общения подростка с виртуальным миром.

Оцените, сколько времени подросток проводит в Сети, не пренебрегает ли он из-за работы за компьютером своими домашними обязанностями, выполнением уроков, сном, полноценным питанием, прогулками.

Говорите с подростком о том, чем он занимается в Интернете. Социальные сети создают иллюзию полной занятости: чем больше подросток общается, тем больше у него друзей, тем больший объем информации ему нужно охватить – ответить на все сообщения, проследить за всеми событиями, показать себя.
Понаблюдайте за сменой настроения в поведении подростка после выхода из Интернета. Возможно ли проявление таких психических симптомов, как подавленность, раздражительность, беспокойство, нежелание общаться? Из числа физических симптомов можно выделить головные боли, боли в спине, расстройство сна, снижение физической активности, потеря аппетита и другие.

Будьте в курсе, с кем контактирует в Интернете Ваш ребенок, старайтесь регулярно проверять список контактов своих детей, чтобы убедиться, что они лично знают всех, с кем они общаются.

Объясните, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, и т.д.).

Если по электронной почте или другим каналам кто-то направляет подростку угрозы и оскорбления, то лучше всего сменить электронные контакты.

Проинформируйте подростка о самых распространенных методах мошенничества и научите его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете.

Если подросток расстроен чем-то увиденным (например кто-то взломал его профиль в социальной сети) или попал в неприятную ситуацию (потратил ваши или свои деньги в результате Интернет-мошенничества), постарайтесь его успокоить и вместе с ним разберитесь в ситуации: что привело к такому результату, какие неверные действия совершил сам подросток, а где вы не рассказали ему о правилах безопасности в Интернете.

Если ситуация связана с насилием в Интернете по отношению к подростку, то необходимо выяснить информацию об агрессоре, выяснить историю взаимоотношений подростка и агрессора, выяснить, существует ли договоренность о встрече в реальной жизни; узнать, были ли такие встречи, и что известно агрессору о подростке (реальное имя, фамилия, адрес, телефон, учебное заведение), жестко настаивайте на избегании встреч с незнакомцами, особенно без свидетелей, проверьте все новые контакты подростка за последнее время.

Если вы не уверены в оценке серьезности произошедшего или подросток недостаточно откровенен с вами или вообще не готов идти на контакт, или вы не знаете как поступить в той или иной ситуации, тогда обратитесь к специалисту (телефон

доверия, «горячая линия» и др.), где вам дадут рекомендации о том, куда обратиться, если требуется вмешательство других служб и организаций (МВД, МЧС и др).

Рекомендации - как распознать интернет- и игровую зависимость
(http://www.google.ru/goodtoknow/familysafety/advice/)

Сегодня в России все более актуальны проблемы так называемой «интернет-зависимости» (синонимы: интернет-аддикция, виртуальная аддикция) и зависимости от компьютерных игр («геймерство»). Первыми с ними столкнулись врачи-психотерапевты, а также компании, использующие в своей деятельности Интернет и несущие убытки, в случае если у сотрудников появляется патологическое влечение к пребыванию онлайн.

Как выявить признаки интернет-зависимости у подростка:

Оцените, сколько времени он проводит в Сети, не пренебрегает ли он из-за работы за компьютером своими домашними обязанностями, выполнением уроков, сном, полноценным питанием, прогулками.

Поговорите с ребенком о том, чем он занимается в Интернете. Социальные сети создают иллюзию полной занятости – чем больше ваш ребенок общается, тем больше у него друзей, тем больший объем информации ему нужно охватить – ответить на все сообщения, проследить за всеми событиями, показать себя. Выясните, поддерживается ли интерес вашего ребенка реальными увлечениями, или же он просто старается ничего не пропустить и следит за обновлениями ради самого процесса. Постарайтесь узнать, насколько важно для ребенка общение в Сети и не заменяет ли оно реальное общение с друзьями.

Понаблюдайте за сменой настроения и поведением вашего ребенка после выхода из Интернета. Возможно проявление таких психических симптомов как подавленность, раздражительность, беспокойство, нежелание общаться. Из числа физических симптомов можно выделить головные боли, боли в спине, расстройства сна, снижение физической активности, потеря аппетита и другие.

Если вы обнаружили возможные симптомы интернет-зависимости у своего ребенка, необходимо придерживаться следующего алгоритма действий:

Постарайтесь наладить контакт с ребенком. Узнайте, что ему интересно, что его беспокоит и так далее.

Не запрещайте ребенку пользоваться Интернетом, но постарайтесь установить регламент пользования (количество времени, которые ребенок может проводить онлайн, запрет на сеть до выполнения домашних уроков и прочее). Для этого можно использовать специальные программы родительского контроля, ограничивающие время в Сети.

Ограничьте возможность доступа к Интернету только своим компьютером или компьютером, находящимся в общей комнате, – это позволит легче контролировать деятельность ребенка в сети. Следите за тем, какие сайты посещает ребенок.

Попросите ребенка в течение недели подробно записывать, на что тратится время, проводимое в Интернете. Это поможет наглядно увидеть и осознать проблему, а также избавиться от некоторых навязчивых действий, например от бездумного обновления странички в ожидании новых сообщений.

Предложите своему ребенку заняться чем-то вместе, постарайтесь его чем-то увлечь. Попробуйте перенести кибердеятельность в реальную жизнь. Например, для многих компьютерных игр существуют аналогичные настольные игры, в которые можно играть всей семьей или с друзьями, при этом общаясь друг с другом вживую. Важно, чтобы у ребенка были не связанные с Интернетом увлечения, которым он мог бы посвящать свое свободное время.

Дети с интернет-зависимостью субъективно ощущают невозможность обходиться без Сети. Постарайтесь тактично поговорить об этом с ребенком. При случае обсудите с ним ситуацию, когда в силу каких-то причин он был вынужден обходиться без Интернета.

Важно, чтобы ребенок понял – ничего не произойдет, если он на некоторое время выпадет из жизни интернет-сообщества.

В случае серьезных проблем обратитесь за помощью к специалисту.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Парошин, А. А. Информационная безопасность: стандартизированные термины и понятия : Методическое пособие к курсу “Технология защиты информации” [Электронный ресурс] / А.А. Парошин. - Владивосток : Изд-во ДВГУ, 2010. - 216 с. Режим доступа: http://bezopasnik.org/article/book/20.pdf
2. Полат, Е.С. Проблема информационной безопасности в образовательных сетях Рунет [Электронный ресурс] / Лаборатория дистанционного обучения Института содержания и методов обучения РАО. - Режим доступа: http://distant.ioso.ru/library/publication/infobez.htm
3. Дети в информационном обществе. Моя безопасная сеть: Интернет глазами детей и подростков [Электронный ресурс] / Региональный общественный Центр интернет-технологий; Фонд развития интернет // Информационный бюллетень Года Безопасного Интернета в России. - 2009. Выпуск 1. - Режим доступа: http://www.fid.su/upload/journal-1.pdf
4. Угрозы [Электронный ресурс] // Энциклопедия информационной безопасности. - Режим доступа: http://www.securelist.com/ru/encyclopedia
5. Руководящие указания для детей и молодых людей по защите в онлайновой среде [Электронный ресурс] / Международный союз электросвязи (ITU) - Режим доступа: http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/children/gl-child-2009-r.pdf
6. Безмалый В.Ф. Обеспечение безопасности детей при работе в Интернет [Электронный ресурс] / В. Ф. Безмалый. - Режим доступа: http://www.ifap.ru/library/book331.pdf
7. Компьютерная безопасность // Энциклопедия безопасности: онлайн-версия книги [Электронный ресурс] / В. И. Громов, Г. А. Васильев. - Режим доступа: http://www.opasno.net/rd419.html
8. Информационная безопасность детей: проблемы и пути решения : Аналитический отчет. Пособие для педагогов, психологов, родителей и всех заинтересованных сторон [Электронный ресурс] / Ш. Смагулова, Н. Байтугелова, Т. Наурызбаев. Центр исследования Сандж; Министерство образования и науки Республики Казахстан; Комитет по охране прав детей. - Астана, 2010. - 119 с. http://www.bala-kkk.kz/fileadmin/user_upload/images/Informacija_bezopasnost_rus..pdf
9. Защита компьютера от вирусов, конфиденциальность личных данных и безопасность в сети [Электронный ресурс] / Центр безопасности Microsoft - Режим доступа: http://www.microsoft.com/ru-ru/security/default.aspx
10. Безопасный Интернет для детей: законодательство, советы, мнения, международный опыт [Электронный ресурс] / Российская ассоциация электронных коммуникаций. - Режим доступа: http://i-deti.org/
11. Пойманные одной сетью: Социально-психологическое исследование представлений детей и взрослых об интернете [Электронный ресурс] / Г. В. Солдатова, Е. Ю. Зотова, А. И. Чекалина, О. С. Гостимская. - М., 2011. - 176 с. Режим доступа: http://detionline.com/assets/files/research/caught_by_net.pdf
12. Борьба с вредоносными программами [Электронный ресурс] / Служба технической лаборатории Касперского. Режим доступа: http://support.kaspersky.ru/viruses
13. Галатенко, В.А. Основы информационной безопасности: Учебный курс Интернет - университета информационных технологий (ИНТУИТ) [Электронный ресурс] / В.А. Галатенко. - Режим доступа: http://www.intuit.ru/department/security/secbasics/

ПРИЛОЖЕНИЯ

Приложение 1.

Тестирование по теме “Направления информационной безопасности”
(для обучающихся в системе профессионального образования)

Укажите один или несколько ответов

Вопрос 1. Укажите направления защиты для обеспечения информационной безопасности:	a)	правовая защита
	b)	организационная защита
	c)	инженерно-техническая защита
	d)	информационная защита
Вопрос 2. Укажите, к какому направлению информационной безопасности пользователя относятся программные средства	a)	Логическая защита
	b)	правовая защита
	c)	организационная защита
	d)	инженерно-техническая защита
Вопрос 3. Приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации относятся к ...	a)	Аппаратные средства инженерно-технической защиты
	b)	Физические средства инженерно-технической защиты
	c)	Криптографические средства инженерно-технической защиты
	d)	Организационные средства инженерно-технической защиты
Вопрос 4. Предупреждение, выявление, обнаружение, пресечение и восстановление – это характеристики защитных действий …	a)	по направлениям
	b)	по способам действий
	c)	по ориентации
	d)	по характеру
Вопрос 5. Организационная защита обеспечивает…	a)	охрану, режим и работу с документами
	b)	регламентацию использования технических средств безопасности

		и информационно-аналитической деятельности по выявлению внутренних и внешних угроз деятельности пользователя
	c)	использование программных средств безопасности по выявлению внутренних и внешних угроз деятельности пользователя
Вопрос 6. Применяются ли организационные средства защиты ПЭВМ и информационных сетей при подготовке и контроле работы пользователей?	a)	да
	b)	нет
Вопрос 7. Регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого либо ущерба исполнителям – это …	a)	правовая защита
	b)	организационная защита
	c)	инженерно-техническая защита
	d)	информационная защита
Вопрос 8. Укажите, какие способы физической защиты могут использоваться для доступа к программным продуктам…	a)	система опознавания по голосу
	b)	система опознавания по почерку
	c)	система опознавания по отпечаткам
	d)	система логической организации данных
Вопрос 9. Использование различных технических средств, препятствующих нанесению ущерба деятельности пользователя – это …	a)	правовая защита
	b)	организационная защита
	c)	инженерно-техническая защита
	d)	информационная защита
Вопрос 10. Специальные законы, другие нормативные акты, правила,	a)	правовая защита

процедуры и мероприятия, обеспечивающие защиту на правовой основе – это …		
	b)	организационная защита
	c)	инженерно-техническая защита
	d)	информационная защита
Вопрос 11. Организационная защита включает:	a)	Организацию использования технических средств
	b)	Организацию работы по анализу внутренних и внешних угроз
	c)	Организацию работы с документами
	d)	Организацию работы с пользователями
Вопрос 12. Применяются ли организационные средства защиты ПЭВМ и информационных сетей при хранении и использовании документов и других носителей (маркировка, регистрация, определение правил выдачи и возвращения, ведение документации и др.)	a)	да
	b)	нет

Ключ: 1-a,b,c; 2-d; 3-a; 4-b; 5-a,b; 6-a; 7-b; 8-a,b,c; 9-c; 10-a; 11-a,b,c,d; 12-a

Приложение 2.

Тест «Условия развития информационной безопасности студентов и учащихся»
(для преподавателей)

Установите соответствие

1.	Сущность сформированности информационной безопасности студента	1.	состояние защищенности жизненно важных интересов личности, проявляющееся в умении выявлять и идентифицировать угрозы информационного воздействия и умении скомпенсировать негативные эффекты информационного воздействия
2.	Информация представляет угрозу при определенных условиях. Целью создания таких условий	2.	целенаправленная теоретическая подготовке педагогов по проблеме информационной безопасности через организацию системы семинаров, программы которых имеют модульную структуру и реализуются с использованием современных средств обучения в интерактивном режиме;

3.	Угроза информационной безопасности	3.	педагогически направляемый процесс развития у подростка знаний об информационной угрозе и умения противостоять ей для минимизации последствий психического и нравственного воздействия.
4.	Информационная безопасность	4.	системная и целенаправленная работе с родителями.
5.	Дополнительное условие развития информационной безопасности учащихся	5.	вопросы организации и проведения занятий, содержательный и психолого-педагогический компоненты данных занятий (направленность на формирование умения выявлять информационную угрозу и умения адекватно реагировать на нее; организацию занятия преимущественно в игровой форме с включением разных видов деятельности и применением опорного конспекта);
6.	Психолого-педагогические условия развития информационной безопасности учащихся	6.	манипуляция сознанием и психикой личности.
7.	Организационно-педагогические условия развития информационной безопасности учащихся	7.	совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства в информационной сфере.
8.	Процессуально-технологическое условие развития информационной безопасности студентов	8.	в умении выявлять информационную угрозу; определять степень ее опасности; уметь предвидеть последствия информационной угрозы и противостоять им.
9.	Содержательное условие развития информационной безопасности студентов	9.	организация взаимодействия педагога и учащихся на основе принципов педагогики гуманизма, готовности учителя принять позицию ребенка, проявлении уважения к самостоятельности личности учащегося;
10.	Информационная безопасность студента	10.	темы и проблемы, раскрывающие смысл информационной безопасности, угрозы, исходящей от информации из различных источников, и специфику угроз,

			исходящих из разных источников;

Ключ: 1-8; 2-6; 3-7; 4-1; 5-4; 6-9; 7-2; 8-5; 9-10; 10-3

Приложение 3.

Тест «Ребенок и интернет (информационная безопасность)»
(для родителей)

Установите соответствие

1.	· Нарушение осанки · Нагрузка на зрение · Различные виды излучений · Компьютерная зависимость	1.	Негативные последствия информационного воздействия: этические проблемы
2.	· НЕ сообщаете личную информацию (имя, адрес, телефон, место учебы), · НЕ встречаетесь с кем-либо из онлайн без разрешения родителей, · НЕ открываете электронное письмо от неизвестных отправителей · НЕ отправляйте свою фотографию по Интернету незнакомцам.	2.	Негативные последствия информационного воздействия: проблемы здоровья
3.	· подготовку сознания детей к противодействию негативным информационным воздействиям; · формирование информационной грамотности (навыки конструктивного мышления); · развитие способности к анализу и критическому восприятию информации; · обучение навыкам и способности отличать качественную и некачественную (ложную, деструктивную) информацию	3.	Негативные последствия информационного воздействия: проблемы обучения
4.	Переутомление, психологическая зависимость, соматические заболевания, снижение работоспособности и др.	4.	Факторы риска при работе ребенка на компьютере
5.	· Парольная защита · С помощью модуля ОС Windows «родительский контроль» · С помощью настройки специальных программ (например: программа Цензор) · Ограничение времени работы ребенка с компьютером	5.	Правила работы ребенка с интернетом
6.	Переоценка нравственных норм, снижение интереса к искусству, чтению, проблемы поведения – перенос образцов поведения из виртуальной действительности в реальную и др.	6.	Средства и методики блокировки негативного воздействия направленные на:

7.	Снижение интереса к обучению, отсутствие времени, перегрузка излишней информацией, низкая успеваемость	7.	Способы защиты ребенка для обеспечения информационной безопасности

Ключ: 1-4; 2-5; 3-6; 4-2; 5-7; 6-1; 7-3

Приложение 4

Викторина для студентов “Безопасный интернет”

http://gagadget.com/contest/softkey/

Наш совет: чтобы правильно ответить на вопросы викторины, вам стоит посетить сайты: softkey.ua и kaspersky.ru. Там вы найдете не только ответы на вопросы, но и узнаете массу полезной информации.

1. Как определить, что ваш компьютер заражен?
    1. Друзья получают от вас по электронной почте сообщения, которых вы не посылали
    2. Компьютер часто зависает либо программы начинают выполняться медленнее обычного
    3. На диске исчезают или изменяют название файлы и папки
    4. Компьютер издает неожиданные звуки, воспроизводимые в случайном порядке
    5. Все вышеперечисленное
2. Что нужно сделать в первую очередь, если компьютер подвергся атаке?
    1. Сделать несколько глубоких вдохов и принять витамины
    2. Съесть не менее двух шоколадок
    3. Вызвать милицию и скорую помощь, в особенно сложных случаях еще и пожарных
    4. Отключить компьютер от интернета
    5. Выключить до приезда специалистов монитор
3. Клавиатурный шпион – это:
    1. Агент спецслужб, в служебные обязанности которого входит просмотр переписки пользователей
    2. Сотрудник, ведущий протокол собраний и набирающий текст сразу на клавиатуре, удаленно подключенной к компьютеру
    3. Программа, отслеживающая ввод пользователем паролей и пин-кодов
    4. Юридический термин, используемый для обозначения правонарушений, связанных с информационной безопасностью
    5. Все вышеперечисленное
4. Какая программа была самой популярной за последние полгода?

1. Kaspersky Internet Security 2010
2. ESET NOD32 Antivirus
3. Антивирус Касперского 2010
4. Microsoft Windows 7 Professional Edition
5. Kaspersky Mobile

5. Какую цель преследует такая угроза как фишинг?

    1. Перенаправлять любые запросы пользователя в браузере на хакерский сайт о рыбалке
    2. Довести пользователя до самоубийства путем постоянного вывода сообщения «купи рыбу!»
    3. Организовать отправку от имени зараженного пользователя приглашения в гости тёще по электронной почте каждый раз, когда он собирается с друзьями на рыбалку
    4. Обманным путем выудить у пользователя данные, позволяющие получить доступ к его учетным записям
    5. Использование вод мирового океана для глобального распространения вредоносных вирусов

6. Что делают при помощи ботнетов?

    1. Устраивают гладиаторские бои роботов
    2. Выполняют вредоносные действия, используя сеть, состоящую из зараженных компьютеров пользователей
    3. Перенаправляют запросы поисковых роботов
    4. Защищают компьютер от атак злоумышленников
    5. Поддерживают оживленную беседу с блондинками в чатах

7. Троянская программа опасна тем, что:

    1. Проникает на компьютер под видом полезной программы и выполняет вредоносные действия без ведома пользователя
    2. Вынуждает пользователя возвращать долги данайцев
    3. Ищет на диске какого-то коня, снижая производительность системы
    4. Постоянно читает вслух «Илиаду» Гомера без выражения
    5. Обладает всеми вышеперечисленными возможностями

8. Чем отличается компьютерный вирус от компьютерного червя?

    1. Ничем, это одно и тоже
    2. Червь не выполняет вредоносных действий
    3. Черви могут делиться, вирусы - нет
    4. Вирус не является самостоятельным файлом
    5. Вирус способен заразить человека, червь - нет

9. Почему беспроводная сеть нуждается в защите?

1. Воздух содержит много вредных микробов, вирусов и инфекций
2. Снижается скорость работы с одновременным ростом счетов провайдера интернета
3. Хакеры получают за взлом обычной сети 1 балл, за взлом беспроводной – 3
4. Это распространенное заблуждение, беспроводная сеть не нуждается в защите
5. Незащищенная беспроводная сеть расходует значительно больше электричества

10. Когда необходима покупка антивирусного ПО?

1. В случае если компьютер заражен, и работа остановилась
2. В следующем году, если поднимут стипендию
3. Перед приездом бабушки
4. На день святого Валентина
5. Сразу после покупки нового компьютера, перед подключением к интернету

Ключ: 1-e; 2-d; 3-c; 4-a; 5-d; 6-b; 7-a; 8-d; 9-b; 10-e

Приложение 5.

Анкета для студентов "Информационная безопасность"

ФИО.....группа.....дата.....

1. Слышали ли вы о кодексе поведения в интернете?
а) да
б) нет
2. Всегда ли вы его соблюдаете?
а) да
б) нет
3. Какие сайты Вы чаще всего посещаете?
а) развлекательные
б) информационные и образовательные
в) социальные сети
г) интернет-магазины
д) игровые порталы
е) форумы и блоги
4. Какие эмоции Вы чаще всего испытываете во время пользования интернетом?
а) радость
б) удивление
в) тревогу
г) разочарование
д) интерес
е) доверие
ж) другие
5. Как часто в интернете Вы размещаете подробную информацию о себе и своих родственниках (адрес, телефон, фото и т. д.)
а) никогда
б) иногда
в) часто
6. Сколько времени в сутки Вы пользуетесь интернетом?
а) меньше 1 часа
б) 1- 2 часа

в) 3-4 часа
г) больше 4-х часов
7. Для каких целей чаще всего Вы используете интернет?
а) для общения
б) для учёбы
в) для развлечения
8. Как ты думаешь, должны ли родители контролировать сайты, которые ты посещаешь?
а) я не против
б) меня это не интересует
в) я категорически против

Приложение 6.

Анкета для педагогов ”Информационная безопасность”

ФИО.....дата.....

1. Проводите ли Вы мероприятия для студентов, ориентированные на повышение их компьютерной грамотности и безопасности?
а) да
б) нет
2. Кто в образовательном учреждении должен разрабатывать и продвигать стратегию информационной безопасности студентов?
а) преподаватель ИКТ
б) представители администрации
в) все педагоги независимо от уровня ИКТ-компетенции
3. Используете ли Вы в своей работе программы для фильтрации интернет-сайтов?
а) да
б) нет
в) не знаю
4. Знакомы ли Вы с требованиями СанПина при работе с ИКТ, соблюдаете ли Вы данные требования?
а) да
б) нет
в) не всегда
5. Какую стратегию информационной безопасности студентов Вы считаете наиболее эффективной?
а) на сайте учреждения создать страницу с рекомендуемыми сайтами по всем предметам
б) сделать в учреждении доступный кабинет для работы в сети Интернет
в) создать буклеты о безопасной работе в интернете с перечнем рекомендуемых сайтов
г) другое
6. Как вы считаете, чему в большей степени вредит интернет?
а) физическому здоровью студентов
б) психическому здоровью студентов
в) нравственности и культурному развитию студентов
г) успеваемости студентов
7. Попадали ли Вы в ситуацию опасности в интернете и смогли ли решить эту проблему?
а) попадал и смог решить проблему самостоятельно
б) попадал и не смог решить проблему самостоятельно
в) не попадал
8. Участвуете ли Вы сами и вместе со студентами в дистанционных проектах, конкурсах, викторинах?
а) участвую только сам
б) участвую только со студентами
в) участвую сам и со студентами
г) не имею такой практики

9. С кем чаще всего Вы общаетесь в социальных сетях?
а) с друзьями и родственниками
б) со студентами
в) с родителями студентов
г) с коллегами

Приложение 7.

Анкета для родителей “Информационная безопасность”

ФИО.....группа.....

1. Какие меры по информационной безопасности вашего ребёнка вы предпринимаете?
а) установили родительский контроль
б) проверяете в браузере журнал посещённых ребёнком интернет-страниц
в) проверяете почту, читаете форумы, посещаете страницы ребёнка в социальных сетях
г) постоянно рассказываете ребёнку об интернет-угрозах
д) другое

2.Контролируете ли Вы количество времени, проведённое ребёнком за компьютером дома?
а) всегда
б) иногда
в) никогда

3. Разговаривали ли Вы со своим ребенком о возможных угрозах, исходящих от интернета?
а) да
б) нет
в) сам о них не знаю

4.Кто, по Вашему мнению, должен нести ответственность за информационную грамотность Ваших детей?
а) родители
б) педагоги
в) сами дети

5. С какой целью используется компьютер ребенком дома?
а) общение в социальных сетях
б) игры и просмотр фильмов
в) подготовка к экзаменам
г)поиск и использование дополнительной учебной информации
д)для участия в интернет-конкурсах и проектах
е) другое.

6. Как влияет компьютер и интернет на ваши отношения с ребенком?
а) вызывает конфликты и споры в семье
б) улучшает Ваши отношения
в) никак не отражается на Ваших отношения

7. Какие меры вы принимаете, чтобы ограничить время пребывания ребенка за компьютером?
а) запрещаете, спорите
б) объясняете, убеждаете
в) отключаете компьютер
г) изменяете финансирование
д) другое

8. Известны ли вам адрес и телефон горячей линии по приему сообщений о противоправном контенте и поведении в интернете?
а) известны и Вы ими пользовались
б) известны, но Вы ими не пользовались
в) не известны, хотелось бы узнать

Приложение 8.

Тест для родителей на наличие игровой интернет-зависимости их ребёнка

Поставьте в соответствующую графу один балл за каждый вопрос, на который вы ответили положительно

Вопросы	Балл
1. Много ли времени ребенок проводит за компьютером, игровой панелью, планшетом, карманным персональным компьютером, смартфоном, играя в компьютерные игры?	
2. Легко ли он прекращает игру по вашему требованию?	
3. Часто ли бывают ситуации, когда ребенок прячется от вас и играет в компьютерные игры?	
4. Часто ли он рассказывает вам о персонажах из компьютерных игр и игровых ситуациях?	
5. Часто ли ребенок с друзьями обсуждает игровые ситуации?	
6. Изменился ли резко его внешний вид, одежда?	
7. Появились ли у него странные и нетипичные предметы: меч, плащ, необычные аксессуары, обувь?	
8. Просит ли он у вас обновить компьютер? Сделать его мощнее, быстрее?	
9. Просит ли ребенок деньги на игры или на непонятные вам цели?	
10. Изменились ли резко его привычки?	

Если сумма баллов дает больше 5, то вам надо обратить внимание на возможную игровую зависимость вашего ребенка!

Приложение 9.

Тест для студентов «Компьютерная зависимость»

(Юрьева, Л. Н., Больбот, Т. Ю. Компьютерная зависимость: формирование, диагностика, коррекция и профилактика: Монография. — Днепропетровск: Пороги, 2006. - 196 с.)

1. Как часто Вы ощущаете оживление, удовольствие, удовлетворение или облегчение, находясь за компьютером (в сети)?
   (1)- никогда (2)- редко (3)- часто (4)- очень часто
2. Как часто Вы предвкушаете пребывание за компьютером (в сети), думая и размышляя о том, как окажетесь за компьютером, откроете определенный сайт, найдете определённую информацию, заведете новые знакомства?
   (1)- никогда (2)- редко (3)- часто (4)- очень часто
3. Как часто Вам необходимо всё больше времени проводить за компьютером (в сети) или тратить все больше денег для того, чтобы получить те же ощущения?
   (1)- никогда (2)- редко (3)- часто (4)- очень часто
4. Как часто Вам удаётся самостоятельно прекратить работу за компьютером (в сети)?
(4)- никогда (3)- редко (2)- часто (1)- очень часто
5. Как часто Вы чувствуете нервозность, снижение настроения, раздражительность или пустоту вне компьютера (вне сети)?
(1)- никогда (2)- редко (3)- часто (4)- очень часто
6. Как часто Вы ощущаете потребность вернуться за компьютер (в сеть) для улучшения настроения или ухода от жизненных проблем?

(1)- никогда (2)- редко (3)- часто (4)- очень часто

7. Как часто Вы пренебрегаете семейными, общественными обязанностями и учебой из-за частой работы за компьютером (пребывания в сети)?

(1)- никогда (2)- редко (3)- часто (4)- очень часто

8. Как часто Вам приходится лгать, скрывать от родителей или преподавателей количество времени, проводимого за компьютером (в сети)?

(1)- никогда (2)- редко (3)- часто (4)- очень часто

9. Как часто существует актуализация или угроза потери дружеских и/или семейных отношений, изменений финансовой стабильности, успехов в учёбе в связи с частой работой за компьютером (пребыванием в сети)?

(1)- никогда (2)- редко (3)- часто (4)- очень часто

10. Как часто Вы отмечаете физические симптомы, такие как: онемение и боли в кисти руки, боли в спине, сухость в глазах, головные боли; пренебрежение личной гигиеной, употребление пищи около компьютера?

(1)- никогда (2)- редко (3)- часто (4)- очень часто

11. Как часто Вы отмечаете нарушения сна или изменения режима сна в связи с частой работой за компьютером (в сети)?

(1)- никогда (2)- редко (3)- часто (4)- очень часто

Оценка результатов:

15 баллов и менее — 0 % риска развития компьютерной зависимости;

16-22 балла — стадия увлеченности;

23-37 баллов — риск развития компьютерной зависимости (необходимость проведения профилактических программ в последующем);

более 38 баллов — наличие компьютерной зависимости!

Полезные ссылки

1. http://www.zapret-info.gov.ru/ - Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено
2. zapret-info@rsoc.ru – адрес электронной почты Единого реестра доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено
3. http://content-filtering.ru/ - Интернет-СМИ “Ваш личный Интернет”
4. http://www.calameo.com/read/0017774253dd6440a1f92 - презентация для родителей “Медиабезопасность школьников” (автор - Тимина Н. В.)
5. http://www.vt.ru/konkurs/works - конкурсные работы “Безопасный интернет”
6. http://nsportal.ru/shkola/vneklassnaya-rabota/library/klassnyi-chas-virtualnoe-obshchenie - разработка классного часа “Виртуальное общение”
7. http://fiit.ucoz.ru/index/socialnye_servisy/0-11 - сайт кафедры ФиИТ Балашовского института (филиала) ФГБОУ ВПО "Саратовский государственный университет имени Н.Г. Чернышевского". Раздел Интернет-помощники - Социальные сервисы
8. http://www.psyhelp.ru/internet/test.php - онлайн-тест на Интернет-зависимость

Сведения об авторах

- Ерофеева Анастасия Олеговна, ассистент кафедры физики и информационных технологий, Балашовский институт (филиал) ФГБОУ ВПО "Саратовский государственный университет имени Н.Г. Чернышевского", e-mail: nastyaerofeeva@mail.ru
- Кульков Александр Александрович, заместитель директора по УПР ГБОУ СПО ВО “Ковровский промышленно-гуманитарный техникум”, e-mail: vahmistr63@mail.ru

- Мурылева Галина Александровна, преподаватель информатики и ИКТ ГБОУ НПО Владимирской области “Профессиональное училище № 10” г. Муром, e-mail: gcyc1@list.ru
- Никишина Татьяна Павловна, преподаватель физики и информатики ГБОУ СПО ВО “Муромский промышленно-гуманитарный техникум”, tatiana.nickischina@gmail.com
- Тимина Наталья Владимировна, социальный педагог, преподаватель психологии и педагогики, ГБОУ СПО ВО “Муромский педагогический колледж” , г. Муром, e-mail: timina2005@rambler.ru
- Топоркова Наталия Ивановна, методист МАОУ ДПО ИПК г. Новокузнецк, e-mail: ipktopni@rambler.ru