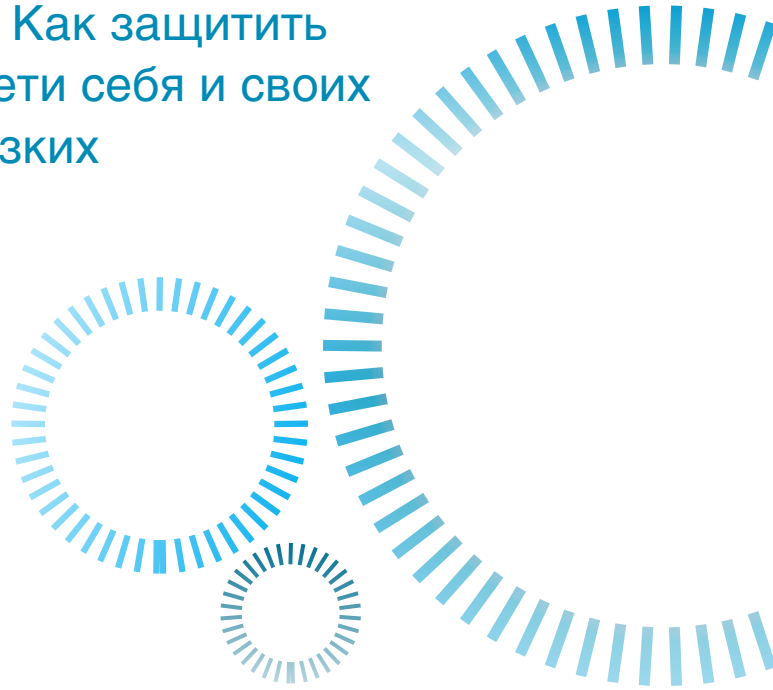
Навыки профессиональной и личной эффективности

А.А. Гладкий

Интернет-безопасность, или Как защитить в Сети себя и своих близких



2017, Москва
Педагогический университет
«Первое сентября»

Гладкий Алексей Анатольевич

Интернет-безопасность,
или Как защитить в Сети себя и своих близких

Педагогический университет
«Первое сентября», 2017. – 32 с.

Учебно-методическое пособие

Редактор С.В. Яковлева
Корректор О.Е. Русакова
Обложка И. Лукьянов
Иллюстрации фотобанк shutterstock
Компьютерная верстка Н.П.Чернявской

Подписано в печать 03.08.2017.
Формат 60 × 90 1/16. Гарнитура Charter, Helios.
Печ. л. 2,0.
Тираж 1000. Заказ №
Педагогический университет «Первое сентября»,
ул. Киевская, 24, Москва, 121165.
http://edu.1september.ru

Введение

Интернет опасен — это аксиома, которую нельзя забывать. Наиболее беззащитны дети и подростки, но попасть в неприятность может и умудренный опытом человек.

Малейшая небрежность — и в лучшем случае вы лишаетесь денег, в худшем — получаете проблемы с законом, психикой, карьерой, теряете семью и друзей, можете остаться без жилья и средств к существованию и даже совершить суицид.

Интернет требует бдительности. Самые опасные места — социальные сети, тематические форумы и чаты, порносайты, торрент-трекеры, ресурсы для совершения онлайн-покупок и платежей. Серьезные неприятности можно получить даже в ходе обычной переписки по электронной почте.

Профессиональные сетевые злодеи моментально овладевают вниманием беспечных обывателей, парализуют их волю и отпускают хватку только тогда, когда «выжмут» из человека все, что им требуется (секретную информацию, деньги, обещание и пр.). Причем почти всегда жертва не подозревает, что полностью лишена возможности самостоятельного принятия решений и действует по чужой указке во вред себе и своим близким.

Вывод прост: каждый пользователь интернета должен уметь защитить себя и своих детей от сетевых опасностей и противостоять киберпреступникам.

О том, как это сделать, вы узнаете после изучения данного курса.

Чего нужно бояться в интернете

Сетевые атаки беспрерывны, агрессивны и беспощадны. интернет изобилует вирусами, электронными шпионами и навязчивой рекламой, кишит хакерами, вымогателями и скрытыми наблюдателями, в нем полно извращенцев и прочих опасных личностей.

Пресловутая интернет-анонимность существует только для злоумышленников, которые умеют прятаться профессионально и эффективно. Рядовые пользователи мгновенно идентифицируются независимо от своего желания, после чего могут находиться под беспрерывной слежкой со стороны государства, частных лиц и организаций, а также представителей преступного мира.

Вся информация, которую вы оставляете на форумах, в социальных сетях, чатах и прочих интернет-ресурсах, мгновенно анализируется, а при необходимости — тиражируется. Это дает заинтересованным лицам массу сведений о вашей личности и роде занятий, финансовом положении, а также о предпочтениях, явных или скрытых желаниях, страхах и опасениях, и т.п.

«Группы риска» традиционны: прежде всего это дети, неопытные пользователи, легко внушаемые и наивные люди. Однако есть немало печальных примеров, когда попавший под профессиональное воздействие опытный человек с твердым ха-

рактером и устойчивой психикой послушно выполняет поступающие из Сети команды или становится жертвой тщательно спланированных обстоятельств.

НЕЖЕЛАТЕЛЬНЫЕ ЗНАКОМСТВА

Виртуально общение (особенно в чатах и на форумах) неприятно тем, что зачастую невозможно узнать, кто на самом деле находится по ту сторону монитора. Во многих случаях личность собеседника остается тайной.

Поэтому даже за самым привлекательным сетевым образом может скрываться крайне неприятный и опасный персонаж. Вот наиболее распространенные последствия общения с подобными личностями:

- втягивание в тоталитарную секту;
- полная или частичная потеря сбережений;
- разглашение секретной информации (от пин-кодов и паролей до подробностей интимной жизни);
- попытки насилия со стороны интернет-знакомого, с которым была договоренность о личной встрече (в лучшем случае это будет обычный грабеж, в худшем можно нарваться на маньяка, которые часто ищут жертв в Сети).

Если интернет-знакомство зашло дальше обычного общения на форуме или в чате и вы планируете развивать его на будущее — поговорите с собеседником через Skype с включенным режимом видео. Это не поможет узнать его реальный род занятий и понять истинные намерения — но, по крайней мере, вы сможете идентифицировать его визуально.

ШАНТАЖ И ВЫМОГАТЕЛЬСТВО

Формы интернет-шантажа и поводы для его осуществления разнообразны. Большинство обывателей наивно полагают, что у них, как у законопослушных граждан, отсутствуют тайны, которые могут заинтересовать вымогателей.

Однако никого не обрадует публикация подробностей интимной жизни (с указанием ФИО) на популярном форуме или размещение телефона с фотографией на сайте фривольных знакомств (с последующим уведомлением супруга/супруги). Есть варианты и попроще, например — дать объявление о по-

иске работы от имени человека, а потом сообщить об этом его начальству.

Массу информации для вымогателей может дать почтовый ящик жертвы. Взломать его несложно — это делают даже дилетанты. Поэтому при ведении электронной переписки не затрагивайте темы, разглашение которых может сделать вас уязвимым.

Достаточно эффективными являются примитивные формы шантажа, рассчитанные на доверчивых и наивных обывателей. Типичный пример — появление всплывающего окна, в котором от имени правоохранительных органов содержится требование заплатить штраф за посещение экстремистских ресурсов, запрещенных торрент-трекеров, порнографических сайтов и т.п., причем для перечисления денег даются реквизиты электронного кошелька.

СЛЕЖКА, ШПИОНАЖ, СКРЫТОЕ НАБЛЮДЕНИЕ

Слежка в интернете ведется за всеми без исключения. Она может быть сравнительно безобидной — например, когда осуществляется с социально-исследовательскими или рекламно-маркетинговыми целями.

Догадаться о ней несложно: после посещения тематического ресурса на экране начинают появляться соответствующие рекламные предложения.

В частности, если вы вчера на форуме обсуждали ремонт автомобиля — сегодня на мониторе промелькнет информация о станциях техобслуживания и о продаже запчастей. Если общались по поводу поступления ребенка в институт — отобразится реклама репетиторов, если советовались по вопросам дрессировки собак — вам будут предложены новые виды собачьего корма, и т.д.

Этим занимаются маркетинговые агентства: подобная реклама может раздражать — но в целом данный вид слежки сравнительно безобиден.

Но в любом случае факт того, что за вами следят, всегда неприятен. Основная опасность в данном случае исходит от:

- **современных смартфонов**. Многие модели (включая самые модные и «раскрученные» девайсы) незаметно шпионят за собственным владельцем — например, запоминая, где и что он фотографировал, с кем и на каких ресурсах общался и т.д.
- **социальных сетей**. Именно здесь представители преступного мира берут информацию, необходимую для кражи, шантажа, вымогательства и иных видов посягательства. Это делается элементарно, поскольку беспечные обыватели сами публикуют полезные для злоумышленников фотографии (из окна своей квартиры), делятся планами на отпуск, личной информацией, особенностями работы, расписанием детей и пр.
- **форумов, чатов и электронной переписки**. Существует перечень выражений и слов, употребление которых моментально вызывает соответствующий интерес со стороны специальных служб. Далее всё зависит от развития ситуации: например, часто человека склоняют к сотрудничеству, используя компрометирующие его материалы (причем они могут быть получены в ходе специально спланированной провокации). Компромат может касаться работы, личной жизни, а также проблем с законом (если жертва вольно или невольно совершила наказуемое деяние).

Следует исходить из того, что любые заверения владельцев веб-ресурсов об анонимности аккаунтов и электронных адресов пользователей и защите их от постороннего доступа несостоятельны. Во-первых, они обязаны открыть любой аккаунт по первому требованию спецслужб, а во-вторых — современные хакеры умеют взламывать практически любую защиту.

КРАЖА ПАРОЛЕЙ, ПИН-КОДОВ, ПРОЧЕЙ СЕКРЕТНОЙ ИНФОРМАЦИИ

Получение прав доступа позволяет злоумышленникам пользоваться чужими аккаунтами и электронными адресами, а также воровать деньги, подписывать от чужого имени электронные документы и т.д.

Во многих случаях жертвы сами проявляют беспечность при вводе и хранении пин-кодов, паролей, номеров кредитных карт и т.п. Однако хакеры способны похищать эту информацию, внедряя на компьютер специальные программы-шпионы.

Чаще всего для этого используются так называемые кейлоггеры — клавиатурные шпионы. Это программы, которые перехватывают всю вводимую пользователем информацию и моментально отсылают ее по указанному злоумышленником адресу.

Некоторые из них активизируются только при посещении соответствующих ресурсов: интернет-магазинов, сайтов для совершения онлайн-платежей, страниц интернет-банкинга и т.д. И после того как пользователь вводит идентификационные данные — они сразу перехватываются и попадают к преступникам, которые моментально блокируют доступ к аккаунту, выводят деньги и т.д.

ИНТЕРНЕТ-ЗАВИСИМОСТЬ

Проблема актуальна не только для детей: многие взрослые также способны практически беспрерывно «зависать» в Сети, игнорируя работу, семью, друзей и полностью выпадая из реального социума. Такие люди психологически переходят в виртуальную реальность, теряя способность адекватно воспринимать и оценивать ситуацию, принимать решения, отвечать за поступки и т.д.

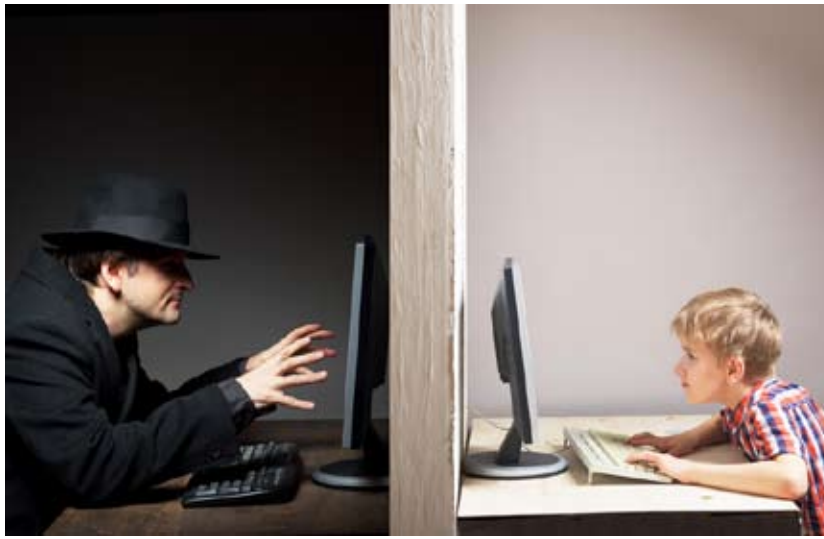
Данная проблема настолько серьезна, что термин «интернет-зависимость» перешел из педагогической и социально-общественной сфер в медицинскую плоскость. Большая опасность в том, что люди впадают в невменяемое состояние незаметно, а избавить их от этой болезни без посторонней помощи практически нереально.

ВНИМАНИЕ

Патологическая привязанность к интернету сопоставима с зависимостью от казино, наркотиков или алкоголя. Общая черта заключается в том, что человек практически полностью теряет волю и не может отказаться от того, к чему успел привыкнуть.

В результате невозможность проверить электронную почту или обновить свою страницу в социальной сети оборачивается настоящей истерикой, а в некоторых случаях становится поводом для суицида.

Интернет-зависимость — распространенная причина семейных драм и разводов, полной или частичной потери сбережений, утраты контроля над детьми, увольнений с работы и прочих серьезных неприятностей. Во многих случаях сетевых фанатиков удается вернуть к нормальной жизни только после вмешательства высококвалифицированного психолога (за услуги которого придется выложить немалую сумму), а также после приема мощных транквилизаторов и прочих дорогостоящих лекарств.



Практическое задание

- Вспомните, с какими интернет-угрозами сталкивались или теоретически могут столкнуться вы или ваши близкие (особенно дети). Смоделируйте перечисленные в данном разделе ситуации применительно к себе и определите, как вы поступите в каждом конкретном случае. Проанализируйте свои ответы. К каким выводам вы пришли в результате выполнения задания? Зафиксируйте их.

Самозащита в интернете: просто и эффективно

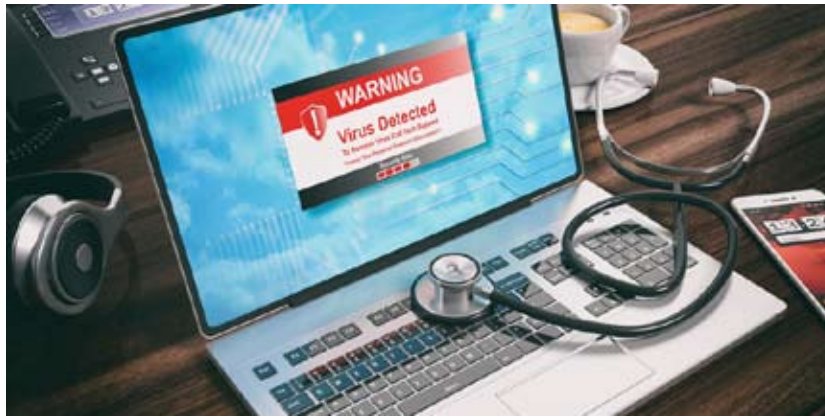
Каждый выход в интернет можно сравнить с посещением многолюдных мест в период эпидемии гриппа или с одиночной ночной прогулкой по бандитскому району. Вы можете подцепить вирус или шпионскую программу, быстро лишиться денег, потерять доступ к своим почтовым ящикам и интернет-банкингу, попасть под наблюдение, стать жертвой шантажа и т.д.

И если в реальной жизни реально ограничить свое посещение нежелательных мест, то без интернета сегодня обойтись нельзя. Поэтому соблюдение хотя бы элементарных мер сетевой безопасности столь же обязательно, как и правил личной гигиены.

БОРЬБА С ВИРУСАМИ. БОЛЕЗНЬ ЛЕГЧЕ ПРЕДУПРЕДИТЬ, ЧЕМ ИЗЛЕЧИТЬ

Интернет кишит компьютерными вирусами и шпионскими программами (SpyWare). Они могут рассылаться по почте, распространяться в социальных сетях, передаваться с помощью привлекательных ссылок и т.д.

Главная опасность вирусов в том, что они способны полностью парализовать компьютер и даже вывести его из строя.



Шпионские программы опасны тем, что могут использоваться как средство получения материалов для вымогательства и шантажа, а также для похищения паролей, пин-кодов, номеров кредитных карт и прочей конфиденциальной информации.

Для защиты используйте надежные антивирусные и антишпионские программы. Без них выходить в интернет нельзя — иначе компьютер моментально превратиться в рассадник вредоносного программного обеспечения.

ВНИМАНИЕ

Опасность еще и в том, что зараженный личный ПК или ноутбук могут незаметно для его владельца использоваться для противоправных действий. Например, без ведома хозяина с его компьютера будут массово рассылаться экстремистские материалы, призывы к участию в несанкционированных мероприятиях или свержению законной власти, реклама запрещенных ресурсов и пр. В подобных ситуациях невиновный человек может получить серьезные проблемы с законом, поскольку доказать свою непричастность к противоправным действиям сложно.

Наиболее опасными с точки зрения заражения компьютера вирусами или шпионскими программами являются:

- **Сайты эротической или порнографической направленности.** Посещение подобных ресурсов для компьютера столь же опасно, как для человека — ведение беспорядочной половой жизни: риск заражения максимален, последствия непредсказуемы.
- **Сайты с пиратским контентом.** Многие из них являются рассадниками огромного количества вирусов, причем для заражения компьютера не обязательно что-то скачивать — достаточно лишь зайти на сайт.
- **Социальные сети.** Здесь распространение вредоносного ПО приобрело массовый характер, чему способствует беспечность пользователей (люди, не задумываясь, делятся с собеседниками зараженными ссылками, приложениями и т.п.).

Основные правила безопасности

- Имейте мощные защитные программы от известных разработчиков.
- Не переходите по ссылкам из личных сообщений (если нужно — копируйте адрес и вставляйте его в адресную строку браузера).
- Не посещайте сомнительные ресурсы.
- Не запускайте незнакомые приложения.
- Не открывайте неизвестные вложения к электронным письмам.

СЕКРЕТЫ БЕЗОПАСНОГО ОБЩЕНИЯ

При создании виртуальных знакомств не стоит быстро переносить отношения из интернета в реальную жизнь. Даже с самым приятным собеседником будьте осторожны: в частности, количество предоставляемой ему персональной информации должно соответствовать объему и качеству полученных от него аналогичных сведений.

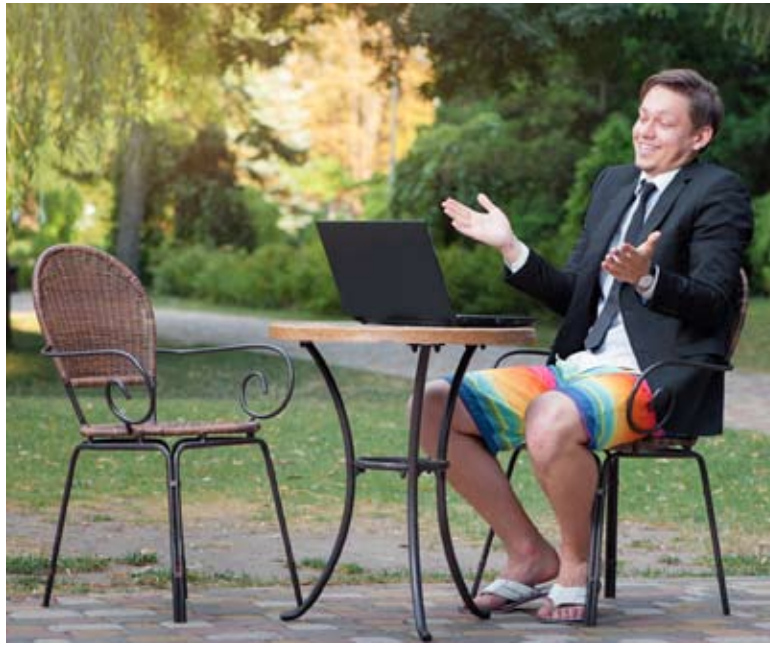
При этом следует всегда помнить, что находящийся по ту сторону экрана человек может делиться недостоверной ин-

формацией, и если проверить ее не представляется возможным — к ней следует относиться критически.

Требуйте домашний телефон, проверьте его принадлежность с помощью справочника (например, через «Желтые страницы»), позвоните по данному номеру и убедитесь, что действительно общаетесь с человеком, с которым познакомились в интернете. Мобильный телефон в данном случае ненадежен, поскольку может принадлежать кому угодно.

При массовом неформальном общении (например, в чатах и на форумах) никогда не раскрывайте реальные имя и фамилию — пользуйтесь исключительно ником, а при регистрации указывайте вымышленные данные. Это несложно, поскольку на подобных ресурсах такая анонимность считается нормой.

Не оставляйте номера домашнего или мобильного телефонов на сайтах знакомств, досках бесплатных объявлений и иных аналогичных порталах. Если требуется вступить с незнакомцем в обычную «бумажную» переписку — не давайте ему домашний адрес, а пользуйтесь арендованным на почте абонентским ящиком.



Доверяйте собственной интуиции: если собеседник вызывает у вас подозрения или настороженность — прекращайте общение и разрывайте контакт. Вескими основаниями для этого являются:

- Неоправданно поспешное (нередко — уже в первых письмах или сообщениях) требование личной встречи.
- Скрытность, нежелание раскрывать о себе даже самую безобидную информацию.
- Назойливость, беспричинная грубость, агрессивная манера общения.
- Сбивчивость письменной или устной речи, ее непоследовательность и нелогичность, запутанность фраз.
- Навязчивое следование определенной теме вплоть до зацикленности, прочие странности в поведении и высказываниях.

Если вы договорились с собеседником о личной встрече — не назначайте ее ни у себя, ни у него дома. Первый «живой» контакт с незнакомцем должен состояться в общественном, активно посещаемом месте: в кафе, выставочном центре, концертном зале, на многолюдной площади и т.п. Лучше появиться заранее и, скрывшись в укромном месте, понаблюдать за человеком, пришедшим на встречу.

КОНТРОЛЬ ЛИЧНОЙ ИНФОРМАЦИИ

О себе в интернете лучше ничего не рассказывать. Если это невозможно — оставляйте минимум информации, причем вовсе не обязательно, чтобы она была достоверной.

В первую очередь это касается социальных сетей. Сегодня подобные ресурсы — настоящий клондайк для представителей преступного мира, а также для работников спецслужб.

Среди элементарных мер безопасности — такая настройка конфиденциальности, чтобы ваш профиль могли видеть только друзья. Это касается абсолютно всего: доступа к фотографиям (особенно если на них — собственная квартира/коттедж и виды из окон, машина, дети и прочие родственники), сообщениям в ленте и на стене, публикаций статусов и прочей информации. А в друзья добавляйте только тех, кого хорошо знаете в реальной жизни.

Принцип работы любой социальной сети построен на стремлении обывателей самим рассказывать о себе, причем как можно подробнее. Чтобы убедиться в этом, достаточно обратить внимание на большое количество необязательных для заполнения параметров: где и кем человек работает, как любит отдыхать, что посещает, какие имеет увлечения и т.д.

Прочти и запомни

Личная страница в социальной сети — это подробное, максимально развернутое и находящееся в свободном доступе досье на ее владельца, которое он составил и бесплатно предоставил на всеобщее обозрение по собственной инициативе.

Большие объемы личной информации похищаются с помощью приложений и игр, созданных для социальных сетей. Особую бдительность следует соблюдать с продуктами, которые просят предоставить полный доступ к персональной странице.

ЗАЩИТА ЭЛЕКТРОННОЙ ПОЧТЫ

Взлом почтового ящика дает злоумышленникам доступ не только к личной переписке, но также к сайтам и прочим сервисам, где данный адрес использовался при регистрации. Они моментально изменят пароль и сразу лишат вас возможности

пользоваться привычными ресурсами, а также смогут несанкционированно действовать от вашего имени.

Поэтому чаще меняйте пароль, избегая простых и банальных комбинаций наподобие последовательных наборов цифр или очевидных вариантов вроде Qwerty, Parol и т.п. Обязательным является сочетание буквенных и числовых символов, причем желательно, чтобы общая длина пароля составляла не менее 10 знаков.

Не разрешайте сохранять его интернет-обозревателю. Никогда не заходите в свой почтовый ящик с посторонних компьютеров или электронных мобильных устройств, которые находятся у друзей, в общественных местах, на работе (включая собственный рабочий ПК) и пр.

Помните непреложное правило: личная почта должна открываться только с личного компьютера или смартфона.

ВНИМАНИЕ

Почтовые ящики, находящиеся в доменной зоне RU (включая те, которые зарегистрированы на авторитетных площадках Yandex, Rambler, Mail и пр.), не могут считаться достаточно надежными и защищенными от взлома. С точки зрения безопасности хорошим вариантом являются электронные адреса от Google.com (Gmail), поддерживающие двухэтапную идентификацию.

При вводе пароля от почтового ящика делайте это с использованием буфера обмена. Наберите требуемую комбинацию в «Блокноте» или иной подобной программе, скопируйте в буфер и вставьте в поле ввода. Этот несложный прием поможет защититься от кражи пароля, осуществляемой с помощью клавиатурного шпиона (кейлоггера).

ЧТО ДЕЛАТЬ, ЕСЛИ ПРОИСХОДИТ НЕЛАДНОЕ

Если вы почувствовали опасность — необходимо предпринять меры, в принципе исключающие ее дальнейшее развитие.

С подозрительными собеседниками прекращайте общение сразу и окончательно, удалив их из всех своих контактов, а при

наличии возможности — отправив в «черный список». Еще лучше — пользоваться «белыми списками»: в этом случае связаться с вами могут только люди, которых вы хорошо знаете. Все остальные потенциальные собеседники не будут иметь возможности написать вам письмо, обратиться через социальную сеть или вести общение иными способами.

Шантаж и вымогательство успешно пресекаются правоохранительными органами. В их распоряжении имеются достаточно эффективные технические и программные средства, позволяющие не только вычислить реальное местонахождение злоумышленников, но и идентифицировать их с последующим задержанием.

Но во многих случаях это может и не потребоваться, поскольку часто шантаж и вымогательство являются обыкновенным блефом. Например, если на экране появляется окно с требованием выслать деньги за разблокировку компьютера — проблема может быть решена переустановкой Windows или запуском антивирусной программы. Требование заплатить штраф за посещение определенных ресурсов (запрещенных торрент-трекеров, порносайтов и т.п.) — явный признак мошенничества, поскольку контролирующие органы в подобных ситуациях действуют совершенно иначе (заводится дело о

правонарушении, высылается повестка и т.д.). Угрозы предоставить компромат на человека его работодателю, супругу/супруге или иным заинтересованным лицам часто ничем реальным не подкреплены.

Если вы чувствуете, что за вами следят — в первую очередь просканируйте компьютер хорошим антишпионским приложением. Следующий этап — быстрое, бесследное и окончательное удаление своих страниц в социальных сетях (не сокрытие или изменение настроек конфиденциальности, а полное удаление!). Быстро заведите новый почтовый ящик и дайте этот адрес людям, с которыми переписывались раньше, — возможно, прежний e-mail уже взломан и пользоваться им нельзя (наблюдатели могут умышленно оставить к нему доступ, чтобы свободно читать переписку).

Практическое задание

- Оцените степень собственной интернет-безопасности. Определите, насколько велики ваши риски быстро лишиться доступа к электронной почте, заразить компьютер вирусом или SpyWare, попасть под слежку, предоставить посторонним конфиденциальную информацию.
- Ответьте на вопросы: Что вы можете сделать, чтобы обезопасить свое пребывание в интернете? Как вы поступите, если почувствуете за собой слежку? Соблюдаете ли вы меры безопасности в социальных сетях?
- Подумайте, как вы можете исключить или минимизировать вероятность получения неприятностей из интернета. Зафиксируйте выводы.

Дети и интернет, или Как не потерять ребенка в Сети

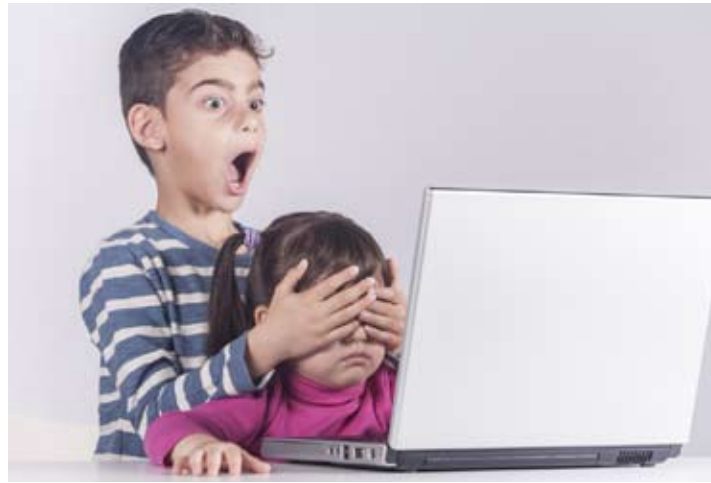
При отсутствии должного контроля со стороны взрослых интернет быстро становится одной из главных опасностей для ребенка. Он вызывает зависимость, становится причиной депрессий и неуверенности в себе, лишает друзей и нормального общения, калечит психику и растлевает, в самых худших случаях — доводит до суицида.

Выпустить ребенка без присмотра в интернет — всё равно, что разрешить ему купаться в открытом море во время шторма. Может, он и выплывает, но высока вероятность печальных последствий.

НУЖНО ЛИ СЛЕДИТЬ ЗА ДЕТЬМИ В ИНТЕРНЕТЕ

Контроль обязателен, и чем сильнее — тем лучше. В данном случае речь не идет о тотальной слежке — но знать жизнь своего ребенка вы обязаны.

Родители, опекуны и прочие ответственные лица по закону должны контролировать детей и знать, чем они занимаются,



как проводят свободное время, с кем общаются и чем интересуются. Это нелегко — современные дети «продвинуты» и способны находить методы обхода запретов. Ситуация осложняется тем, что в интернет сегодня выходят не только с домашних компьютеров, но и с мобильных устройств — смартфонов, планшетов и т.п.

Дома можно ограничить время нахождения ребенка за компьютером, причем находиться при этом рядом — но он может выйти в интернет со своего телефона, будучи вне квартиры (например, в зоне свободного Wi-Fi).

Пользуйтесь функциями родительского контроля, лично блокируйте возможность посещения нежелательных ресурсов. Внедрите на компьютер и смартфон ребенка шпионскую программу — и вы будете знать, какие сайты он посещает, как много времени на них проводит и чем занимается, с кем общается и т.д.

Не стесняйтесь следить за детьми — ничего плохого или позорного в этом нет. Вы и только вы отвечаете за своего ребенка — и именно вы будете жестко корить себя, если с ним что-то случится из-за вашего недосмотра.

Важно

Наблюдение должно быть незаметным — иначе ребенок будет не только разозлен и оскорблен (что вполне естественно — это нормальная реакция любого человека на слежку за собой), но и на эмоциях может наделать глупостей, а вы надолго, если вообще не навсегда, потеряете с ним контакт и лишитесь его доверия.

Тайны от родителей у детей есть всегда — вопрос лишь в том, что это за секреты и насколько их много. *Обязанность взрослых — контролировать те из них, которые могут быть опасными для ребенка.* И процессом незаметной слежки вы никак ребенку не навредите, зато сможете вовремя вмешаться в случае такой необходимости, тем самым защитив его от крупных неприятностей.

А вот принимать правильные решения по результатам наблюдений умеют, к сожалению, далеко не все. Не стоит ругать, наказывать или стыдить мальчика-подростка,

посетившего эротический сайт или девочку, по беспечности вступившую в переписку с потенциально опасным незнакомцем.

Немедленные санкции по факту нелицеприятного, по мнению родителей, поступка — главная и наиболее распространенная ошибка, которая моментально сводит на нет весь эффект от тайного наблюдения за ребенком.

ВНИМАНИЕ

Не ругайте ребенка, если в своей переписке с друзьями он негативно отзывается об учителях, школе, говорит обидные вещи о родителях, употребляет плохие слова и т.п.

По большому счету, большого секрета здесь нет — это свойственно большинству детей, особенно подросткового возраста.

Цель наблюдения за поведением ребенка в интернете — не уличение его в неблаговидных поступках, а защита от серьезных опасностей, в числе которых — склонение к суициду, вымогательство, растление и т.п.

Каждый факт следует проанализировать в спокойной обстановке, каким бы возмутительным он вам ни казался. Понаблюдайте за ребенком дальше: например, если он лишь изредка посещает нежелательные ресурсы (речь не только о «клубничке» — дети могут просматривать ролики сцен казни, съемки медицинских операций и т.п.) — скорее всего, большой опасности в этом нет.

Но если ребенок постоянно и подолгу проводит время на подобных ресурсах — необходимо бить тревогу. Попробуйте вызвать его на более-менее откровенный разговор. Но если вы не уверены, что сможете сделать это ненавязчиво и не выдавая истинных причин для беседы — обратитесь к специалистам (например, к детскому психологу).

Учтите, что дети могут негативно относиться к посещению подобных специалистов и в любом случае скрывают это от сверстников. Действуйте мудро и тактично: например, скажите ребенку, что это необходимо лишь потому, что он стал беспокойным во сне (ворочается, всхлипывает и т.п.). А психологу незаметно для ребенка (это можно сделать непосредственно перед приемом, оставив его в коридоре) сообщите истинную причину посещения.

ВНИМАНИЕ

Все модные нынче разговоры о «недостойности слежки за ребенком», «нарушении его прав на частную жизнь» и т.п. зачастую инициированы теми, кто сам заинтересован в наличии бесконтрольных детей.

Никто лучше родителей не может знать — когда и в чем контролировать конкретного ребенка. Дети все разные: тот же Гайдар в 15 лет командовал полком, а кто-то в этом возрасте не может самостоятельно собрать в школу портфель. Есть дети, которые по характеру рассеянны, наивны, доверчивы — и они нуждаются в усиленном контроле вплоть до совершеннолетия.

Даже если ваш ребенок не по годам самостоятелен (зарабатывает деньги, нянчит младших братьев/сестер, помогает по дому, может один ездить на другой конец города и т.п.) — это не делает его неуязвимым к посягательствам со стороны взрослых, особенно если он знакомится с ними в интернете.

КАК СПАСТИСЬ ОТ «СИНЕГО КИТА»

Сравнительно недавно вся Россия была шокирована серией детских самоубийств, совершенных по указанию злоумышленников из социальных сетей. Самый известный пример — пресловутая группа «Синий кит» из сети Вконтакте.

Проблема осложнялась тем, что суицид совершали дети из благополучных семей, не имевшие проблем со сверстниками, учебой, любящие родителей и уважающие учителей. Стандартных поводов для тревоги (раздражительность, проблемы с друзьями или учебой, потеря аппетита и т.п.) не было — внешне ребенок оставался таким, как и прежде.

Впоследствии выяснилось: это объясняется тем, что причин для расстройства или суицида у погибших детей не было — весь процесс склонения к самоубийству представлен в виде увлекательной игры, в которой последовательно нужно было пройти несколько этапов (последний из них — суицид). Поэтому дети относились к ней как к развлечению, никак не выказывая внешней тревоги.

В настоящее время «Синие киты» и прочие подобные группы быстро блокируются администраторами социальных сетей — но не исключено, что они вновь смогут появляться в той или иной форме. В связи с этим есть несколько рекомендаций, которые помогут защитить ребенка от опасностей.

Тревожный симптом — внезапное появление царапин на теле без видимых причин. Например, если ребенок все выходные просидел дома (не ходил гулять, не играл в футбол, не посещал тренировки), и в это время на его ноге или руке неожиданно появилась глубокая ссадина — не исключено, что это он выполнил одно из заданий куратора «группы смерти».

Обращайте внимание на появление новых татуировок, рисунков и прочих изображений на теле ребенка, в его комнате, школьных тетрадях, в иных местах, которые имеют к нему отношение. Многие погибшие участники «групп смерти» рисовали синих китов или больших бабочек, причем эти изображения могли иметь внушительные размеры — например, на половину стены в детской комнате.

Не подключайте в телефоне ребенка мобильный интернет, а в квартире на ночь отключайте любой доступ к Сети, не давая детям пароль доступа. Днем выпускайте его в Сеть только на определенное время и под присмотром. Многие задания, получаемые от кураторов «групп смерти», необходимо выполнять ночью или ранним утром — когда родители спят. Например, в 4.20 утра детям предлагается просмотреть видеоролик, имеющий агрессивную психологическую направленность — это часто является последним толчком к суициду. Отсутствие в квартире интернета лишит его такой возможности,

Fotos593 / Shutterstock.com

а любые проявления беспокойства по этому поводу могут свидетельствовать о том, что он уже является участником «группы смерти».

В этой связи еще более актуальным становится слежение за детьми, о чем мы уже говорили ранее.

Ни один ребенок даже из самой благополучной семьи не расскажет родителям о том, что он состоит в «группе смерти» — этот вопрос легко решается кураторами, находящими простые и эффективные методы воздействия на детскую психику.

Более того — они запугивают детей, которые по тем или иным причинам решат выйти из «группы смерти» или отказаться от совершения последнего шага — самоубийства. Угрозы примитивны, но действенны: «убьем родителей», «твой младший брат не вернется из садика» и т.п.

Контролируйте своего ребенка и обязательно убедите его в том, что любые угрозы из Сети заслуживают того, чтобы немедленно рассказать о них родителям.

ЧТО ПОКАЗАТЬ РЕБЕНКУ В ИНТЕРНЕТЕ

В Сети есть огромное количество полезных и интересных ресурсов, адресованных детям разных возрастов и предпочтений.

Вы можете показывать им фильмы и мультики, читать с ними увлекательные статьи о природе и Вселенной, изучать в игровой форме иностранный язык, вместе просматривать смешные видеоролики, учиться играть на музыкальных инструментах, готовиться к экзаменам и т.п.

Здесь всё зависит от интересов и потребностей конкретного ребенка: по запросу в поисковике вы получите массу ссылок на бесплатные ресурсы соответствующей тематики.

Кроме этого, в интернете есть достаточно материалов, которые, несмотря на свой шокирующий характер, могут оказаться полезными для детей. Их легко найти на Youtube или на других подобных ресурсах.

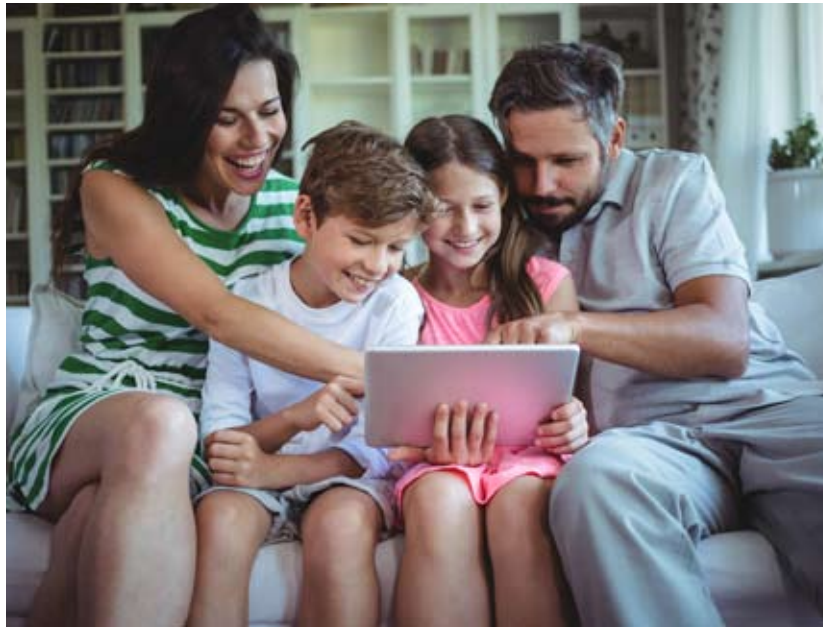
Типичный пример — дорожные аварии. Одно дело — говорить ребенку и необходимости соблюдения ПДД, и другое — наглядно продемонстрировать, как в относительно безобидной ситуации (например, во дворе или даже на пешеходном переходе) машины сбивают детей.

Многие современные дети восхищаются руферами — любителями несанкционированно покорять небоскребы, вышки и прочие высотные сооружения.

Часто подростки мечтают повторить подобные трюки — но нездоровый интерес можно быстро погасить, продемонстрировав впечатляющие и даже шокирующие видеоролики с падениями неудачливых руферов.

Практическое задание

- Знаете ли вы, чем занимаются ваши дети в интернете?
- Какой лимит установлен вами на их пребывание в Сети?
- Можете ли вы сказать, что вероятность посягательств из интернета на психику, здоровье и жизнь ваших детей исключена?
- Подумайте, в чем может заключаться уязвимость именно ваших детей к возможным опасностям со стороны интернет-злоумышленников.
- Каким предложением или фразой их можно заинтересовать, морально обезоружить или запугать?
- Что вы предпримете для того, чтобы спасти детей от возможных интернет-угроз?
- Зафиксируйте выводы.



Помните: полностью запретить ребенку пользоваться интернетом невозможно, да и не нужно.

При должном контроле со стороны взрослых всемирная Сеть не будет угрожать детям, а станет полезной и увлекательной частью их жизни.

Литература

1 *Колисниченко Д.* Анонимность и безопасность в Интернете. От «чайника» к пользователю. СПб.: БХВ-Петербург, 2012.
2 *Мурсалиева Г.* Дети в Сети. Шлем безопасности ребенку в Интернете. М.: АСТ, 2017.
3 *Гладкий А.* Основы безопасности и анонимности во Всемирной сети. М.: Феникс, 2012.

Автор выражает надежду, что предложенный курс был полезен и интересен слушателям. Вопросы и пожелания направляйте по адресу: *alexei.gladki@gmail.com*

ОГЛАВЛЕНИЕ

Гладкий Алексей Анатольевич — автор экономической, бухгалтерской, прикладной литературы. К настоящему времени из-под его пера вышло более 100 книг, большинство из которых за короткий срок выдержали несколько тиражей. Фирменный стиль А.А. Гладкого — простота и доступность изложения, легкость подачи материала, а также множество ценных советов и рекомендаций, основанных на реальных событиях. Все это во многом предопределяет популярность автора у читателей и обеспечивает стабильно высокий спрос на его работы.