ГБУ ДПО СО «Красноярский РЦ»

Словарь интернет-угроз

Автор-составитель:

старший методист

Борисова Н.П.

2016 г.

Аутинг - преднамеренная публикация личной информации ребенка с целью его унизить, при этом произведенная без его согласия. Аутинг может принимать разные формы, при этом опубликованная информация может быть как серьезной, так и незначительной. Даже чтение сохраненных сообщений на телефоне ребенка можно считать аутингом. Личную информацию никогда нельзя разглашать, поэтому родители должны обязательно убедиться, что, если такой случай произойдет с ребенком, он сообщит о кибербуллинге представителям социальной сети, школы или другого учреждения в соответствии с конкретной ситуацией.

Вирусы (Viruses): программы, которые заражают другие программы – добавляют в них свой код, чтобы получить управление при запуске зараженных файлов. Это простое определение дает возможность выявить основное действие, выполняемое вирусом – заражение. Скорость распространения вирусов несколько ниже, чем у червей.

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. Типичный пример фишинга, когда клиенты какой-либо платёжной системы получают сообщения по электронной почте якобы от администрации или службы безопасности данной системы с просьбой указать свои счета, пароли и т.п. При этом ссылка в сообщении ведёт на поддельный сайт, на котором и происходит кража информации. Сайт этот уничтожается через некоторое время, и отследить его создателей в интернете достаточно сложно.

Вредоносные программы — различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред компьютеру и нарушить конфиденциальность хранящейся в нем информации. Подобные программы чаще всего снижают скорость обмена данными с интернетом, а также могут использовать ваш компьютер для распространения своих копий на другие компьютеры, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети. Вредоносное программное обеспечение использует множество методов для распространения и проникновения в компьютеры, не только через внешние носители информации (компакт-диски, флешки и т.д.), но и через электронную почту посредством спама или скачанных из интернета файлов.

Гриферство или грифинг — акт нанесения морального и материального ущерба людям в компьютерных играх. Иными словами, это внутриигровой вандализм.

Груминг – это установление дружеского и эмоционального контакта с ребенком в интернете для его дальнейшей сексуальной эксплуатации. Работают преступники по следующей схеме: лицо, заинтересованное в интимной связи с несовершеннолетним, представляется в сети другим человеком, втирается в доверие к ребенку и настаивает на личной встрече. Последствия для поддавшегося на уговоры ребенка могут быть очень плачевны.

Диссинг - передача или публикация порочащей информации о жертве онлайн. Это делается с целью испортить репутацию жертвы или навредить ее отношениям с другими людьми. Информация может публиковаться в самых разных форматах, от текста до фото, скриншотов или видео. Обидчик всеми силами будет пытаться унизить ребенка, при этом привлекая максимум внимания к этому процессу.

Домогательство - постоянная и умышленная травля при помощи оскорбительных или угрожающих сообщений, отправленных вашему ребенку лично или как часть какой-либо группы. Эта форма кибербуллинга крайне опасна и может привести к серьезным последствиям для ребенка. Эти злонамеренные сообщения могут устрашить ребенка и навредить ему, делая его неуверенным в себе. То, что такие сообщения будут посылаться постоянно, означает, что ребенку

не будет даваться никакой передышки от травли, что делает этот вид кибербуллинга особенно опасным.

Интернет-зависимость — навязчивое желание войти в интернет, находясь офлайн и неспособность выйти из интернета, будучи онлайн. По своим проявлениям она схожа с уже известными формами аддиктивного поведения (например, в результате употребления алкоголя или наркотиков), но относится к типу нехимических зависимостей, то есть не приводящих непосредственно к разрушению организма. По своим симптомам интернет-зависимость ближе к зависимости от азартных игр; для этого состояния характерны следующие признаки: потеря ощущения времени, невозможность остановиться, отрыв от реальности, эйфория при нахождении за компьютером, досада и раздражение при невозможности выйти в интернет. Исследователи отмечают, что большая часть Интернет-зависимых (91 %) пользуется сервисами Интернета, связанными с общением. Другую часть зависимых (9%) привлекают информационные сервисы сети.

Исключение - форма кибербуллинга аналогична бойкоту: жертву намеренно исключают из отношений и коммуникации.

Кетфишинг – форма кибербуллинга, в которой киберхулиган с целью обмана воссоздает профили жертвы в социальных сетях на основе украденных фотографий и других личных данных. Чаще всего обидчики будут пытаться скрыть, кем они на самом деле являются. Они будут использовать информацию, которую ребенок уже разместил в социальных сетях, для создания поддельных личностей. Иногда они ограничатся только фотографией ребенка и используют выдуманное имя, но иногда они могут использовать и всю доступную информацию. Часто бывает сложно понять, зачем обидчик занимается кетфишингом, но в любом случае важно понимать, что эта форма кибербуллинга может серьезно навредить репутации ребенка.

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов. Английское слово буллинг (bullying, от bully — драчун, задира, грубиян, насильник) обозначает запугивание, унижение, травлю, физический или психологический террор, направленный на то, чтобы вызвать у другого страх и тем самым подчинить его себе. Основной площадкой для кибербуллинга в последнее время являются социальные сети. В них можно оскорблять человека не только с помощью сообщений – нередки случаи, когда страницу жертвы взламывают (или создают поддельную на ее имя), где размещают лживый и унизительный контент.

Кибербуллинг- использование силы или влияния, прямо или косвенно, в устной, письменной или физической форме, либо путем демонстрации или иного использования снимков, символов или чего-либо другого в целях запугивания, угроз, травли, преследования или смущения при помощи интернета или других технологий, к примеру, мобильных телефонов.

Кибермошенничество — один из видов киберпреступлений, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.). Отправка любых смс на короткие номера сотовых операторов с последующим списанием средств со счета мобильного телефона сверх указанной ранее суммы либо без получения указанной услуги также является видом кибермошенничества.

Киберпреследование - это преследование человека сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью интернет-коммуникаций. Также, киберпреследование может принимать такие формы, как обмен информацией, контактами или

изображениями, запугивание, подражание, хулиганство (интернет-троллинг) и социальное бойкотирование.

Кибersталкинг - этим термином могут называться попытки взрослых связаться с детьми и подростками через Интернет с целью личной встречи и дальнейшей сексуальной эксплуатации. Эта форма кибербуллинга крайне опасна и может иметь самые серьезные последствия, поэтому по обнаружению необходимо принимать все меры, чтобы немедленно ее остановить.

Контентные риски - материалы (тексты, картинки,аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию. В первую очередь, с таким контентом можно столкнуться на сайтах социальных сетей, в блогах, на торрентах. Но сегодня практически весь интернет - это виртуальное пространство риска.

Незаконный контакт — это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка. Это понятие включает в себя такие интернет-преступления как домогательство и груминг.

Незаконный контент - распространение наркотических веществ через интернет, порнографические материалы с участием несовершеннолетних, призывы к разжиганию национальной розни и экстремистским действиям.

Неэтичный контент - контент, который не запрещен к распространению, но может содержать информацию, способную оскорбить пользователей. Подобное содержимое может распространяться ограниченно (например, "только для взрослых"). Особо опасны сайты, на которых обсуждаются способы причинения боли и вреда, способы чрезмерного похудения, способы самоубийства, сайты, направленные против отдельных групп или лиц. Столкновения с контентными рисками могут иметь негативные последствия для эмоциональной сферы психологического развития, социализации, а также физического здоровья детей и подростков.

Нигери́йские пи́сьма — распространённый вид мошенничества, получивший наибольшее развитие с появлением массовых рассылок по электронной почте (спама). Письма названы так потому, что особое распространение этот вид мошенничества получил в Нигерии, причём ещё до распространения Интернета, когда такие письма распространялись по обычной почте. Однако нигерийские письма приходят и из других африканских стран, а также из городов с большой нигерийской диаспорой (Лондон, Амстердам, Мадрид, Дубай). Рассылка писем началась в середине 1980-х гг. Как правило, мошенники просят у получателя письма помощи в многомиллионных денежных операциях, обещая солидные проценты с сумм. Если получатель согласится участвовать, у него постепенно выманиваются все более крупные суммы денег якобы на оформление сделок, уплату сборов, взятки чиновникам, и т. п..

Обман - киберхулиган обманом пытается завоевать доверие ребенка, чтобы тот рассказал ему какую-либо чувствительную информацию, которую обидчик затем публикует в сети. Обидчик сначала «подружится» с ребенком и обманом вызовет у него ложное чувство безопасности, а потом нарушит созданное доверие и отправит полученную информацию третьим лицам.

Онлайн-шантаж — злоумышленник добывает фотографии или видео, изображающие интимную жизнь своей будущей жертвы, а затем шантажирует, угрожая распространением этих материалов. Чаще всего, целью шантажа является получение новых снимков или видео. Такой вот замкнутый круг. Зачастую злоумышленники получают снимки, взламывая плохо защищенные аккаунты, или заражая устройства вредоносными программами. В результате они получают доступ к галереям или облачным хранилищам своих жертв, а в некоторых случаях и к их веб-камерам. Впрочем, случается что жертва сама отправляет злоумышленнику снимки, поддавшись на его уловки. При этом, ребенок зачастую стыдится рассказать родителям о факте

вымогательства, опасаясь наказания или непонимания с их стороны. Таким образом подросток оказывается в неприятной безвыходной ситуации, которая потенциально может нанести ему глубокую психологическую травму.

Поддельные профили - киберобидчики могут создавать поддельные профили – скрывать то, кем они на самом деле являются, чтобы травить ребенка. Также они могут использовать чужие телефонные номера и адреса электронной почты, чтобы заставить ребенка думать, что им угрожает не обидчик, а кто-то другой. Часто хулиганы используют поддельные профили, потому что боятся, что их личность станет известна.

Потенциально опасные приложения (Riskware): программное обеспечение, не являющееся вирусом, но содержащее в себе потенциальную угрозу. При некоторых условиях наличие таких программ на компьютере подвергает ваши данные риску. К таким программам относятся утилиты удаленного администрирования, программы автоматического дозвона на платные ресурсы интернета с использованием Dial Up-соединения и другие.

Программы-маскировщики (Rootkit): это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами. Rootkit'ы также могут модифицировать операционную систему на компьютере и заменять основные ее функции, чтобы скрыть свое собственное присутствие и действия, которые предпринимает злоумышленник на зараженном компьютере.

Программы-рекламы (Adware): программный код, без ведома пользователя включенный в программное обеспечение с целью демонстрации рекламных объявлений. Как правило, программы-рекламы встроены в программное обеспечение, распространяющееся бесплатно. Реклама располагается в рабочем интерфейсе. Зачастую данные программы также собирают и переправляют своему разработчику персональную информацию о пользователе.

Программы-шпионы: программное обеспечение, позволяющее собирать сведения об отдельно взятом пользователе или организации без их ведома. О наличии программ-шпионов на своем компьютере вы можете и не догадываться. Как правило, целью программ-шпионов является: отслеживание действий пользователя на компьютере; сбор информации о содержании жесткого диска; в этом случает чаще всего речь идет о сканировании некоторых каталогов и системного реестра с целью составления списка программного обеспечения, установленного на компьютере; сбор информации о качестве связи, способе подключения, скорости модема и т.д. Однако данные программы не ограничиваются только сбором информации, они представляют реальную угрозу безопасности. Как минимум две из известных программ – Gator и eZula – позволяют злоумышленнику не просто собирать информацию, но и контролировать чужой компьютер. Другим примером программ-шпионов являются программы, встраивающиеся в установленный на компьютере браузер и перенаправляющие трафик. Наверняка вы встречались с подобными программами, если при запросе одного адреса веб-сайта открывался совсем другой.

Программы-шутки (Jokes): программное обеспечение, не причиняющее компьютеру какого-либо прямого вреда, но выводящее сообщения о том, что такой вред уже причинен, либо будет причинен при каких-либо условиях. Такие программы часто предупреждают пользователя о несуществующей опасности, например, выводят сообщения о форматировании диска (хотя никакого форматирования на самом деле не происходит), обнаруживают вирусы в незараженных файлах и т.д.

Прочие опасные программы: разнообразные программы, которые разработаны для создания других вредоносных программ, организации DoS-атак на удаленные сервера, взлома других компьютеров и т. п. К таким программам относятся хакерские утилиты (Hack Tools), конструкторы вирусов и т.д.

Секстинг - отправление сообщений интимного характера. Это может быть просто текстовая переписка, фотографии или видео. Преступники находят контакты подростка и связываются с ним, чтобы получить эротические фотографии или видео. Фото или видео можно отправить через любой мессенджер или социальную сеть. Это позволяет получать от детей интимные снимки, не вступая с ними в контакт в реальной жизни. Помимо прочего злоумышленники зачастую неплохо понимают детскую психологию и могут убедить ребенка, что все, что он делает, якобы безобидно. Такие фото и видеоматериалы могут стать частью «личной коллекции» педофила, но гораздо чаще они оказываются на ресурсах, распространяющих детскую порнографию. Борьба с сайтами, содержащими детскую порнографию, ведется давно и активно, и найти их в открытом доступе сейчас очень сложно. Тем не менее, это не означает, что они исчезли. Детская порнография остается одним из направлений криминального бизнеса и, очевидно, приносит производителям контента немалые деньги.

Спам (Spam): анонимная, массовая почтовая корреспонденция нежелательного характера. Так, спамом являются рассылки политического и агитационного характера, письма, призывающие помочь кому-нибудь. Отдельную категорию спама составляют письма с предложениями обналичить большую сумму денег или вовлекающие в финансовые пирамиды, а также письма, направленные на кражу паролей и номеров кредитных карт, письма с просьбой переслать знакомым (например, письма счастья) и т. п. Спам существенно повышает нагрузку на почтовые сервера и повышает риск потери информации, важной для пользователя.

Троллинг - намеренная провокация при помощи оскорблений или некорректной лексики на интернет-форумах и в социальных сетях. Тролли будут лично нападать на жертву и стараться унизить ее. Основная задача троллинга – разозлить жертву и заставить ее прибегнуть, так же как и сам тролль, к оскорблениям и некорректной лексике. Тролли могут тратить долгое время в поисках особенно уязвимой жертвы. Как правило, тролли получают положительные эмоции за счет унижения других.

Троянские программы (Trojans): программы, которые выполняют на поражаемых компьютерах несанкционированные пользователем действия, т.е. в зависимости от каких-либо условий уничтожают информацию на дисках, приводят систему к "зависанию", воруют конфиденциальную информацию и т.д. Данный класс вредоносных программ не является вирусом в традиционном понимании этого термина (т.е. не заражает другие программы или данные); троянские программы не способны самостоятельно проникать на компьютеры и распространяются злоумышленниками под видом "полезного" программного обеспечения. При этом вред, наносимый ими, может во много раз превышать потери от традиционной вирусной атаки.

Фарминг — один из видов сетевого мошенничества, похожий на фишинг и основанный на использовании фальшивых веб-сайтов и краже конфиденциальной информации. Отличие фарминга от фишинга заключается в следующем: в аферах с фишингом пользователь переходит на фиктивный веб-сайт, попадаясь на уловку в виде фальшивого электронного письма или ссылки, в то время как фарминг работает за счет перенаправления жертв на фиктивный веб-сайт даже тогда, когда пользователь ввел правильный веб-адрес. Чаще всего это происходит с веб-сайтами банков или интернет-магазинов.

Фишинг (Phishing) – почтовая рассылка, целью которой является получение от пользователя конфиденциальной информации как правило финансового характера. Такие письма составляются таким образом, чтобы максимально походить на информационные письма от банковских структур, компаний известных брендов. Письма содержат ссылку на заведомо ложный сайт, где пользователю предлагается ввести, например, номер своей кредитной карты и другую конфиденциальную информацию.

Флейминг — «спор ради спора», процесс обмена сообщениями в местах многопользовательского сетевого общения (чаты, Интернет-форумы, социальные сети и др.). Данное явление представляет собой словесную войну, которая зачастую не имеет отношения к первоначальной причине дискуссии, спора. Иногда применяется в контексте троллинга, но чаще всего флейм вспыхивает из-за недоразумения, обиды на виртуального собеседника.

Фрейпинг - форма кибербуллинга, в которой обидчик каким-либо образом получает контроль над учетной записью ребенка в социальных сетях и публикует нежелательный контент от его имени.

Черви (Worms): данная категория вредоносных программ для распространения использует сетевые ресурсы. Название этого класса было дано исходя из способности червей "переползать" с компьютера на компьютер, используя сети, электронную почту и другие информационные каналы. Также благодаря этому черви обладают исключительно высокой скоростью распространения. Черви проникают на компьютер, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Помимо сетевых адресов часто используются данные адресной книги почтовых клиентов. Представители этого класса вредоносных программ иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

Использованные интернет-ресурсы:

1. Защита детей https://kids.kaspersky.ru/

2. Дети онлайн http://detionline.com/helpline/rules/parents

3. Родителям об информационной безопасности
https://sites.google.com/site/roditelidetibezogfsnost/kommunikacionnye-riski/kiberpresledovanie

4. Википедия https://ru.wikipedia.org

5. Norton by Symantec https://ru.norton.com/cybercrime-pharming/

6. Лаборатория Касперского https://support.kaspersky.ru/614