Интернет-риски

Все опасности интернет-среды мы объединяем в четыре крупные группы рисков:

Контентные риски.

Контентные риски — это материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д. Столкнуться с ними можно практически везде. Это и сайты, и социальные сети, и блоги, и торренты, и видеохостинги, фактически все, что сейчас существует в Интернете. Зачастую подобный материал может прийти от незнакомца по почте в виде спама или сообщения.

Негативные контентые материалы можно условно разделить на:

- Незаконные, к которым могут относиться: детская порнография (включая изготовление, распространение и хранение); наркотические средства (изготовление, продажа, пропаганда употребления), все материалы, имеющие отношение к расовой или религиозной ненависти (экстремизм, терроризм, национализма и др.), а также ненависти или агрессивного поведения по отношению к группе людей, отдельной личности или животным), азартные игры и т.д.

Внутреннее законодательство каждой страны предусматривает различные виды наказания за распространение такой информации. В Российском законодательстве есть возможность в соответствии со статьями Уголовного кодекса РФ привлечь к административной и уголовной ответственности за распространение подобного негативного контента владельцев сайтов, а также авторов таких электронных текстов и видеопродукции.

- Неэтичные, противоречащие принятым в обществе нормам морали и социальным нормам.

Подобные материалы не попадают под действие уголовного кодекса, однако могут оказывать негативное влияние на психику столкнувшимися с ними человека, особенно ребенка. Примерами таких материалов могут служить широко распространенные в сети изображения сексуального характера, в том числе и порнография, агрессивные онлайн игры, азартные игры, пропаганда нездорового образа жизни (употребление наркотиков, алкоголя, табака, анорексии, булимии), принесения вреда здоровью и жизни (различных способов самоубийства, аудионаркотиков, курительных смесей), нецензурная брань, оскорбления, и др. Информация, относящаяся к

категории неэтичной может быть также направлена на манипулирование сознанием и действиями различных групп людей.

Контентные риски связаны с другими типами рисков Сети. Например, просмотр тех или иных видео-материалов может привести к заражению компьютера вирусами и потере важных данных. Очень многие распространители подобного негативного контента преследуют цель заразить компьютер, чтобы в дальнейшем иметь возможность манипулировать данными и действиями зараженного компьютера. Пропаганда негативных материалов также может идти через социальные сети, блоги, различные форумы. В данном случае контентные риски пересекаются с коммуникационными.

Коммуникационные риски.

Коммуникационные риски связаны с межличностными отношениями интернет-пользователей и включают в себя риск подвергнуться оскорблениям и нападкам со стороны других. Примерами таких рисков могут быть: незаконные контакты (например, груминг), киберпреследования, кибербуллинг и др. Для подобных целей используются различные чаты, онлайн-мессенджеры (ICQ, Google talk, Skype и др.), социальные сети, сайты знакомств, форумы, блоги и т.д.

Даже если большинство пользователей существующих чат-систем (веб-чатов или IRC) обладают добрыми намерениями, существует, к сожалению, растущее число людей, использующих эти беседы со злым умыслом. В некоторых случаях они хотят обманом заставить детей выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам в интернете и др. В других случаях они могут оказаться педофилами в поисках жертвы. Выдавая себя за сверстника и устанавливая дружеские отношения с ребенком, они выведывают о нем много информации и понуждают к личной встрече.

Оказаться жертвой намного проще, чем кажется. Каждый участник той или иной социальной сети может признаться, что хотя бы один раз ему приходило непристойное предложение от неизвестного человека. Это беда не только социальных сетей. На любом популярном форуме, в блоговом сообществе и чате появляются такие участники, которые хамят и оскорбляют других участников.

Коммуникационные риски включают в себя «незаконный контакт» и «киберпреследование» (или кибер-буллинг).

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.

Домогательство — причиняющее неудобство или вред поведение, нарушающее неприкосновенность частной жизни лица. Такое поведение может заключаться в прямых или косвенных словесных оскорблениях или угрозах, недоброжелательных замечаниях, грубых шутках или инсинуациях, нежелательных письмах или звонках, показе оскорбительных или унизительных фотографий, запугивании, похотливых жестах, ненужных прикосновениях, похлопываниях, щипках, ударах, физическом нападении или в других подобных действиях.

Груминг — установление дружеских отношений с ребенком с целью изнасилования.

Злоумышленник нередко общается в интернете с ребенком, выдавая себя за ровесника либо ребенка немного старше. Он знакомится в чате, на форуме или в социальной сети с жертвой, пытается установить с ним дружеские отношения и перейти на личную переписку. Общаясь лично («в привате»), он входит в доверие к ребенку, пытается узнать номер мобильного и договориться о встрече.

Киберпреследование (или кибер-буллинг) — это преследование пользователя сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью различных интернет-сервисов. Также, киберпреследование может принимать такие формы, как обмен информацией, контактами; запугивание; подражание; хулиганство (интернет-троллинг); социальное бойкотирование. По форме буллинг может быть не только словесным оскорблением. Это могут быть фотографии, изображения или видео жертвы, отредактированные так, чтобы быть более унизительными.

Подобный унизительный контент может исходить от одного человека или группы людей по одному или нескольким электронным контактам жертвы, на электронный ящик или в сообщениях онлайн-мессенджеров. Распространены также случаи преследования в социальных сетях или на подобных им ресурсах. При этом помимо рассылки оскорбительных сообщений и вывешивания унизительных материалов, изображений или видеозаписей, буллер может также взломать профиль или страницу жертвы и организовать спам-рассылку по всем контактам жертвы.

К сожалению, кибербуллинг — очень распространенное явление среди российских подростков. Каждый пятый ребенок может признать, что подвергался буллингу онлайн или в реальной жизни. И это беда не только России, она распространена во всем мире. Но в России дети становятся жертвами буллинга в интернете так же часто, как и в реальной жизни.

Нередко кибербуллинг берет начало в отношениях с реальными людьми, и в этом случае, жертва знает своих оскорбителей. Когда же буллинг берет свое в интернете, всегда важно удостовериться, чтобы он не перерос в реальное насилие над ребенком.

Электронные риски.

Электронные (кибер-) риски — это возможность столкнуться с хищением персональной информации, риск подвергнуться вирусной атаке, онлайн-мошенничеству, спам-атаке, шпионским программам и т.д. Вредоносное ПО (Программное Обеспечение) использует широкий спектр методов для распространения и проникновения в компьютеры, не только через компакт-диски или другие носители, но и через электронную почту посредством спама или скачанных из Интернета файлов.

К вредоносным программам относятся вирусы, черви и «троянские кони» – это компьютерные программы, которые могут нанести вред вашему семейному компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с Интернетом и даже использовать ваш компьютер для распространения своих копий на компьютеры ваших друзей, родственников, коллег и по всей остальной глобальной Сети. Защита в социальных сетях — это задача, которая не так давно стала актуальна для их пользователей. Буквально несколько месяцев назад, взлом страниц в социальных сетях превратился в один из основных способов распространения спама в Интернете.

В частности, теперь вирусное ПО (программное обеспечение), которое рассылает спам в социальной сети может быть установлено на ваш компьютер с любого сайта. И от вашего лица могут регулярно рассылаться абсолютно любые сообщения, избавиться от которых не поможет ни одна защита самого сайта. Хотя бы просто по той причине, что в этом случае потребуется не защита вашей страницы, а современное антивирусное программное обеспечение. Поэтому не забывайте обновлять свою антивирусную программу и следить за защитой своего компьютера.

К сожалению, вероятность наткнуться на подобные вредоносные программы очень велика. Помимо негативного воздействия на компьютер и мобильное устройство, можно стать жертвой еще одного вида кибер-преступления — кибер-мошенничества. В самом широком смысле мошенничество — это умышленный обман или злоупотребление доверием с целью получения какой-либо выгоды.

Мошенничество в сети Интернет (кибермошенничество) — один из видов киберпреступления, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер

незаконно получает доступ и каким-либо образом использует личную информацию пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.), с целью причинить материальный и финансовый ущерб.

Потребительские риски.

Потребительские риски – злоупотребление в интернете правами потребителя. Включают в себя: риск приобретения товара низкого качества, различные поделки, контрафактная и фальсифицированная продукция, потеря денежных средств без приобретения товара или услуги, хищение персональной информации с целью кибер-мошенничества, и др.

Также дети, зачастую совершая онлайн покупки, могут растратить значительные суммы своих родителей, если каким-либо способом имели или получили к ним доступ.

Одним из самых распространенных видов данного типа рисков является мошенничество — это умышленный обман или злоупотребление доверием с целью получения какой-либо выгоды. Мошенничество, как правило, является преступлением.

Поскольку мошенничество в сети интернет совершается с помощью различных технических средств и разнообразного количества программ, то некоторые его виды могут быть отнесены и к группе электронных рисков, а часть к группе коммуникационных, поскольку включает в свою схему установления более близкого контакта с жертвой в течение какого-либо времени (например, с помощью электронных писем и смс, которые могут привести и к реальным встречам с мошенниками).