# ОПОРНЫЙ ПЛАН-КОНСПЕКТ

В настоящее время Интернет является неотъемлемой частью жизни большинства людей. И дети не стали исключением, в связи с чем остро стоит проблема их безопасности в глобальной сети, а также необходимость формирования у них представлений о виртуальном и реальном мире. Одной из задач органов внутренних дел является разработка инновационных подходов, позволяющих не только научить ребенка безопасному поведению, но и заинтересовать его в дальнейшем делиться полученными знаниями со сверстниками и использовать их в жизни.

Средний возраст для первого погружения в неизведанные пучины интернета – это 5-6 лет. В настоящее время более 80% детей от 7 до 12 лет пользуются Интернетом самостоятельно, что составляет примерно 30% интернет-аудитории страны.

Все это происходит на фоне минимальных познаний у подрастающего поколения по индивидуальному обеспечению собственной информационной безопасности. Как следствие, в течение последних лет число противоправных деяний, совершенных против информационной безопасности, ежегодно увеличивается.

Казалось бы, что это сложные по механизму совершения преступления, однако, 90% совершаются людьми, не имеющими никакого специализированного образования в данной сфере. И если говорить о молодежной аудитории, то половина совершаются лицами от 14 до 24 лет.

В сети Интернет действуют те же законы, те же нравы, те же обычаи, что и в реальной жизни.

При этом учитывая последние общемировые тенденции, в первую очередь, прогнозируется дальнейшее увеличение количества хищений путем использования компьютерной техники (статья 212 УК) и фактов несанкционированного доступа к компьютерной информации (статья 349 УК), совершаемых путем компрометации данных держателей банковских платежных карт посредством фишинга с применением социальной инженерии и взлома учетных записей пользователей в социальных сетях.

## Как не стать жертвой преступлений в социальных сетях

На сегодняшний день в молодёжной среде мы вряд ли найдем тех, кто не был бы зарегистрирован «ВКонтакте», «Фейсбуке», «Инстаграмм», каких-либо тематических форумах или иных площадках для виртуального общения. В целом это норма, ведь человек живет в обществе и стремится общаться. Однако некоторая неопытность, наивность и доверчивость порой приводят к негативным последствиям.

Социальные сети, форумы, блоги – это среда с практически мгновенной скоростью распространения информации и довольно сильным эффектом памяти (содержимое многих социальных ресурсов

индексируется и доступно из поисковиков). Кроме того, растет индекс доверия к этим источникам информации.

Основная проблема социальных сетей – это доверие к тем, кто внесен в список «друзей». Бездумное предложение «дружбы» от неизвестных или малоизвестных людей может привести к драматическим последствиям. Очевидно, что уровень доверия к тем, кто находится в списке «друзей», по определению всегда будет выше, чем к случайным людям. С одной стороны, это хорошо, так как формирует лояльную аудиторию вокруг человека, но с другой стороны, открывает двери для злоумышленников.

«Дружеский» стиль общения, распространенный в социальных сетях, обманчив. Он может создать ложное ощущение, что вокруг только друзья и доброжелатели, с которыми можно делиться любой информацией.

Очень хорошо отсутствие культуры общения, а точнее, наличие антикультуры раскрывает такое явление, как «троллинг».

**На интернет-сленге троллинг** (от анг. trolling –ловля рыбы на блесну) – это намеренно агрессивное, хамское, провокационное, оскорбительное поведение в интернет-дискуссии. Цель тролля (тролль – это тот, кто занимается троллингом) – вывести собеседника из равновесия, разжигание склок в дискуссиях, провоцирование взаимных оскорблений и т.д. Помимо этого, виртуальность вызывает эффект «онлайн-растормаживания», благодаря которому люди позволяют себе в Интернете такое поведение и высказывания, которые никогда бы себе не позволили в реальном мире.

Общение в сети, точно такое же общение, как и в обычной жизни, с той лишь разницей, что дети порой доверяют «виртуальным друзьям» гораздо больше, чем реальным. Особенно это обостряется в тот момент, когда у подростка возникают проблемы в реальной жизни или в общении со сверстниками. В сети очень быстро находятся «сопереживающие» и «советующие». Отсюда и возникают такие известные движения как «Синий Кит» (когда подростка склоняли к совершению самоубийства) или «Колумбайн» (когда ребенка подталкивали на совершение физических расправ над учителями, учащимися или просто незнакомыми людьми).

Зачастую злоумышленники ведут очень долгую и дружескую переписку, находят слабые места, втираются в доверие, становятся лучшим другом или подругой, делают вид, что понимают собеседника лучше всех на свете, а потом, понемногу начинают склонять к тем либо иным действиям, манипулировать или шантажировать. Преследуя эти цели, злоумышленники порой используют фотографии «друзей» из профиля подростка, чтобы создать дубликат страницы этого «друга» и якобы от его имени уже вести переписку.

Обезопаситься от этого можно лишь развивая критичное отношение к собеседникам в сети и их словам, проявляя не меньшую осторожность, чем в обычной жизни. Не следует выставлять всю свою жизнь напоказ, гонясь за мнимой известностью, «лайками» и комментариями и конечно же следует понимать, что слова, написанные в личных сообщениях, отправленное фото и иные сведения, могут стать инструментом, который позволит манипулировать собеседником.

Вторая угроза связана со взломом пользовательских записей социальных ресурсов. И это происходит не потому, что использовались простые пароли (что конечно тоже бывает) или они записывались где-то, грубо говоря «на бумажке» и кто-то мог их «подсмотреть».

Проблема носит более масштабный характер. Источников утечки персональной информации о логинах и паролях пользователей данной социальной сети крайне много и в подавляющем большинстве случаев вина лежит на самих пользователях, которые осуществляли авторизацию на иных ресурсах или в приложениях через свои учетные записи в социальных сетях. Например, для скачивания музыки или видеофайлов, получения мнимого выигрыша. Часть из данных ресурсов были созданы именно для сбора персональной информации.

Посредством взлома злоумышленник может проникнуть в социальную сеть, разослать по ее списку друзей фишинговое (или заведомо ложные) сообщение и получить деньги либо мотивировать получателей к каким-либо негативным действиям. Например, пройти по указанной ссылке и запустить вредоносный код.

**ВСЕГДА:**

будь внимательным, посещая чаты. Даже если в чате написано, что он только для детей, нельзя точно сказать, что все посетители действительно являются твоими ровесниками. В чатах могут сидеть взрослые, пытающиеся тебя обмануть;

спрашивай у родителей разрешения посидеть в чате;

покидай чат, если чье-то сообщение вызовет у тебя чувство беспокойства или волнение. Не забудь обсудить это с родителями;

держи информацию о пароле при себе, никому его не говори;

если услышишь или увидишь, что твои друзья заходят в “небезопасные зоны”, напомни им о возможных опасностях и посоветуй, как им правильно поступить;

будь внимателен при загрузке бесплатных файлов и игр на компьютер, тебя могут обмануть: нажав на ссылку, ты можешь попасть в “небезопасную зону” или загрузить на свой компьютер вирус или программу – шпион;

если получили оскорбляющие сообщения, расскажите об этом родителям;

помни, что если кто-то сделает тебе предложение, слишком хорошее, чтобы быть правдой, то это, скорее всего, обман;

держись подальше от сайтов «только для тех, кому уже есть 18». Такие предупреждения на сайтах созданы специально для твоей же защиты. Сайты для взрослых также могут увеличить твой счет за Интернет.