План-конспект для использования в процессе обучения школьников на тему:

«Основы обеспечения безопасности в сети Интернет и информационном пространстве»

Уже совершенно не секрет, что в настоящее время практически все трудоспособное население нашей страны так или иначе вовлечено в процессы, связанные с ресурсами сети Интернет. Естественно все эти процессы оказывают очень существенное влияние на молодежную среду, проникновение в которую сети Интернет и высоких технологий оценено практически в 100%. В наше время средний возраст для первого погружения в неизведанные пучины интернета — это уже 5-6 лет. В настоящее время более 70% детей от 7 до 12 лет пользуются интернетом самостоятельно, что составляет примерно 20% интернет-аудитории страны.

Все это происходят на фоне в большинстве своем минимальных познаний населения по индивидуальному обеспечению собственной информационной безопасности. Как следствие в течении последних лет число выявленных преступлений, совершенных против информационной безопасности ежегодно прирастает в разы.

Казалось бы, что это сложные по механизму совершения, преступления, однако, 90% таких преступлений совершаются людьми, не имеющими никакого специализированного образования в данной сфере. И если уж говорить о молодежной аудитории, то половина этих

преступлений либо совершена лицами от 14 до 24 лет, либо совершена в отношении них.

Преступность в сети Интернет приобретает все большие масштабы. Изобретаются все новые уловки по выкачиванию денег, практически полная безнаказанность, анонимность преступников, большое количество доверчивых людей – все это подпитывает этот своеобразный «бизнес».

В сети Интернете действуют те же законы, те же нравы, те же обычаи, что и в реальной жизни, в «оффлайне». Это же касается и противоправной деятельности, желание некоторых граждан обогатиться за чужой счет, утвердить собственное «я», получить власть над другими.

Текущий уровень преступности в сфере высоких технологий

В 2019 году в Брестской области продолжила наблюдаться тенденция увеличения числа зарегистрированных преступлений, относящихся к сфере высоких технологий (далее СВТ). В настоящее время в области зарегистрировано 665 высокотехнологичных преступления (в 2018 - 383, +73,6 %). При этом рост преступлений фиксируется как по преступлениям против информационной безопасности (182, АППГ – 127, +43,3%), так и по хищениям с использованием компьютерной техники (483, АППГ - 256, +88,7%).

Справочно: рост высокотехнологичных преступлений отмечается по всей республике (+101,1 %) и присущ каждому региону страны.

Большая доля преступлений в СВТ приходится на территорию обслуживания крупных населенных пунктов, таких как г. Брест, г. Барановичи и г. Пинск. При этом количество зарегистрированных преступлений по линии СВТ в указанных городах выросло примерно в два раза.

Как не стать жертвой преступлений в социальных сетях

На сегодняшний день в молодёжной среде мы вряд ли найдем кого-либо, кто не был бы зарегистрирован «В Контакте», «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 приводит 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, это 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) — доведение собеседника до белого каления, разжигание склок в дискуссиях, провоцирование взаимных оскорблений и т. д. Быть троллем в определенной Интернет-среде — почетно и похвально. Если кому- то кажется, что троллинг — это редкая аномалия, то он сильно ошибается. Троллинг распространен повсеместно, негласно используется в политике и бизнесе. Благодаря анонимности, невидимости, безнаказанности очень многим действительно «в кайф» вызывать ненависть в остальных.

Помимо этого, анонимность, виртуальность вызывают эффект «онлайн-растормаживания». Благодаря этому эффекту люди позволяют себе в Интернете такое поведение, такие высказывания, которые никогда бы себе не позволили в реальном мире.

Общение в сети - это 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). Для этого используются специально созданные группы, а также особые хэштеги — «куратор», увидев их на страничке ребенка, связывается с ним. «Куратор» дает школьнику инструкции: что нужно делать, чтобы присоединиться к смертельной игре. Участники этих «групп смерти» ассоциируют себя с китами — высокоразвитыми животными, которые якобы осознанно совершают массовые самоубийства, выбрасываясь на берег. Способность на самоубийство привязывается к внутренней свободе. Картина издыхающих китов некрасива, и поэтому в сообществах эти «свободные» киты летают. Из групп смерти поклонники «моря китов» и «тихих домов» репостят (пересылают друг другу) видео и графику с летающими китами под медитативные звуки. Детям предлагают пройти экзамен — повредить себя, а потом предоставить фото и видео этого для вхождения в группу.

Зачастую злоумышленники ведут очень долгую и дружескую переписку, находят слабые места, втираются в доверие, становятся лучшим другом/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, злоумышленника порой используют фотографии «друзей» из профиля подростка, чтобы создать дубликат страницы этого «друга» и якобы от его имени уже вести переписку.

Значительную степень опасности носит излишняя наивность и **доверчивость** детей. Например, недавно в семье появился достаточно дорогой ноутбук или телевизор, ребёнок непременно обрадуется и захочет поделиться этой новостью с друзьями и знакомыми в социальной сети. Он легко может на радостях разместить Вконтакте фотографии дорогой покупки, написав при этом в исходных данных профиля свой домашний адрес и похвастаться, в дополнение ко всему прочему, предстоящей поездкой всей семьи на отдых в санаторий. Чем это грозит, понимает абсолютно любой взрослый человек, но далеко не каждый ребёнок.

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.

Вместе с тем, существует целая группа полезных ресурсов, таких как например «Википедия». Посещение этих сайтов намного полезнее для ребёнка, чем решение однотипных школьных задач. Понятно, что не каждый ребёнок будет часами сидеть на этих интернет-ресурсах по доброй воле, но, когда ему придется выполнять домашнее задание или готовится к публичным выступлениям, их помощь будет просто незаменима!

Даже казалось бы совершенно бесполезное зависание ребёнка в социальной сети может иметь положительные стороны, если ребёнок, к примеру, заинтересуется создателями этих самых социальных сетей – Павлом Дуровым (основатель Вконтакте) или Марком Цукербергом (основатель Facebook), изучит их биографию и мышление, захочет подражать им и овладеть их положительными качествами характера.

Вторая угроза связана с 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 его «подсмотреть». Проблемы носит более масштабный характер. Источников утечки персональной информации о логинах и паролях пользователей данной социальной сети крайне много и 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 данной 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 – в частности, пройти по указанной ссылке и запустить вредоносный код.

Таким образом, после совершения несанкционированного доступа к персональным аккаунтам, в течении первых суток зачастую развиваются следующие сценарии:

- злоумышленник, рассылает всем виртуальным «друзьям» потерпевшего просьбу под различными предлогами сообщить реквизиты банковской платежной карты. Это может быть ее фото или просто номер, срок действия и иные реквизиты, при этом, хоть в большинстве своем школьники банковских карт не имеют, но желая помочь «другу» очень часто используют карты своих родственников и друзей. Порой преступники просят просто номер мобильного телефона и либо пытаются похитить со счета телефона деньги или наоборот используют его как промежуточное звено, направляя на этот счет чужие деньги, переводя их затем дальше, чтобы запутать свои следы (практически во всех случаях хищения денежных средств со счетов мобильных телефонов потерпевшие еще сообщали преступнику персональные коды, приходящие в виде смс-сообщений на телефон). Анализ показывает, что не более 20% людей, получивших такие сообщения, связываются с владельцем страницы, что в этой ситуации крайне важно. Чтобы обезопасить себя от этого вида преступлений, что не стоит сообщать никому реквизиты доступной банковской платежной карты или номер мобильного телефона и содержание смс-сообщений, поступающих для подтверждения совершения операции. Ежедневно на территории обрасти фиксируется несколько подобных случаев.

- злоумышленник, изучает содержание переписок потерпевшего и использует их содержание в качестве инструмента для вымогательства денежных средств. Таким образом, инструментом вымогательства становятся личные диалоги на откровенные темы, фотографии, содержащиеся на странице и в диалогах и иные очень личные данные.

Обычно, перед тем как связаться с потерпевшим, преступник делает скриншот списка всех его друзей и близких. Избежать подобного возможно лишь путем регулярной чистки своих диалогов и удаления из сети всей информации, компрометирующего характера.

- злоумышленник, начинает рассылать различного рода порочащую информацию от имени владельца страницы иным пользователям.

В случае обнаружения «взлома» аккаунта, прежде всего следует попытаться восстановить доступ наиболее привычным способом, путем отправки сообщения на «привязанный» номер мобильного телефона или электронную почту, кроме этого следует оповестить друзей и знакомых об инциденте, используя при этом иные социальные сети и мессенджеры. Кроме этого, чтобы в какой-то мере обезопасить себя от взлома, специалисты по безопасности рекомендуют «привязать» страницу социальной сети именно к номеру мобильного телефона, а не к адресу электронной почты, помимо этого в настройках страницы в разделе «Безопасность» подключить услугу «Подтверждение входа». При этом вход на Вашу страницу с неизвестного компьютера или мобильного телефона будет не возможен без знания кода, который автоматически будет выслан на указанный при регистрации страницы номер.

Как не стать жертвой преступлений против информационной безопасности

Основным источником опасности для пользователей компьютеров были и остаются вредоносные программы, которые с развитием сетевых технологий получили новую среду для своего распространения.

Вирусы – это наиболее распространённая угроза для детей в интернете. Взрослый сразу же заметит, что новый видеоклип никак не может иметь расширение *.exe, а письма с заголовками «Вы выиграли 1 000 000 долларов» лучше удалять, не открывая. Для детей, это совсем не очевидный факт, и их любопытство может дорого стоить родителям, когда, например, данными их пластиковых карт воспользуются, скажем, в Индонезии.

Вредоносные программы можно разделить на три группы:

- компьютерные вирусы;
- сетевые черви;
- троянские программы.

Компьютерный вирус - это обычная программа, которая обладает самостоятельно прикрепляться к другим работающим программам, таким образом, поражая их работу. Вирусы самостоятельно распространяют свои копии, это значительно отличает их от троянских программ. Также отличие вируса от червя в том, что для работы вирусу нужна программа, к которой он может приписать свой код;

Скрипт-вирусы и черви - достаточно просты для написания и распространяются в основном посредством электронной почты. Скриптовые вирусы используют скриптовые языки для работы чтобы добавлять себя к новым созданным скриптам или распространяться через функции операционной сети. Нередко заражение происходит по e-mail или в результате обмена файлами между пользователями. Червь это программа, которая размножается самостоятельно, но которая инфицирует при этом другие программы. Черви при размножении не могут стать частью других программ, что отличает их от обычных видов компьютерных вирусов;

Троянские программы - это программы, которые должны выполнять определенные полезные функции, но после запуска таких программ выполняются действия другого характера (разрушительные). Трояны не могут размножаться самостоятельно, и это основное их отличие их от компьютерных вирусов.

Кроме этого, в настоящее время получили широкое распространение и иные программные продукты, носящие вредоносный характер:

Bot-сеть:

Bot-сеть это полноценная сеть в Интернет, которая подлежит администрированию злоумышленником и состоящая из многих инфицированных компьютеров, которые взаимодействуют между собой. Контроль над такой сетью достигается с использованием вирусов или троянов, которые проникают в систему. При работе, вредоносные программы никак себя не проявляют, ожидая команды со стороны злоумышленника. Подобные сети применяются для рассылки СПАМ сообщений или для организации DDoS атак на нужные сервера. Что интересно, пользователи зараженных компьютеров могут совершенно не догадываться о происходящем в сети;

Рекламные программы:

Под рекламными и информационными программами понимаются такие программы, которые, помимо своей основной функции, также демонстрируют рекламные баннеры и всевозможные всплывающие окна с

рекламой. Такие сообщения с рекламой порой бывает достаточно нелегко скрыть или отключить. Такие рекламные программы основываются при работе на поведение пользователей компьютера и являются достаточно проблемными по соображениям безопасности системы.

Бэкдоры (Backdoor):

Утилиты скрытого администрирования позволяют, обходя системы защиты, поставить компьютер установившего пользователя под свой контроль. Программа, которая работает в невидимом режиме, дает хакеру неограниченные права для управления системой. С помощью таких backdoor-программ можно получить доступ к персональным и личным данным пользователя. Нередко такие программы используются в целях заражения системы компьютерными вирусами и для скрытой установки вредоносных программ без ведома пользователя.

Фарминг:

Фарминг - это скрытая манипуляция host-файлом браузера для того, чтобы направить пользователя на фальшивый сайт. Мошенники содержат у себя сервера больших объемов, на таких серверах хранятся большая база фальшивых интернет-страниц. При манипуляции host-файлом при помощи трояна или вируса вполне возможно манипулирование зараженной системой. В результате этого зараженная система будет загружать только фальшивые сайты, даже в том случае, если Вы правильно введете адрес в строке браузера.

Фишинг:

Phishing дословно переводится как "выуживание" личной информации пользователя при нахождении в сети интернет. Злоумышленник при своих действиях отправляет потенциальной жертве электронное письмо, где указано, что необходимо выслать личную информацию для подтверждения. Нередко это имя и фамилия пользователя, необходимые пароли, PIN коды для доступа к счетам пользователя онлайн. С использованием таких похищенных данных, хакер вполне может выдать себя за другое лицо и осуществить любые действия от его имени.

Шпионское ПО:

Шпионы могут переслать личные данные пользователя без его ведома третьим лицам. Шпионские программы при этом анализируют поведение пользователя в сети Интернет, а также, основываясь на собранных данных, демонстрируют пользователю рекламу или pop-up (всплывающие окна), которые непременно заинтересуют пользователя.

Разновидностью вирусов, получившей очень широкое распространение в нашей стране, является блокировщик системы Windows. Вирус проникает на компьютер пользователя (этот процесс может происходить автоматически и незаметно) и добавляет свой код в

автозапуск системы. После перезагрузки компьютера операционная система блокируется, появляется сообщение о необходимости внести некоторую сумму денег (зачастую в виде мнимого штрафа за какие-либо действия в сети) на указанный счет или отправить смс на номер телефона. При этом могут содержаться угрозы об уничтожении данных или привлечении к какой-либо ответственности.

Чтобы не стать жертвой преступлений против информационной безопасности, следует неукоснительно следовать правилам информационной гигиены: не устанавливать программное обеспечение из неизвестных источников, перед открытием электронных писем следует убедиться в отсутствии в них скрытых исполняемых файлов, а также использовать наиболее современную версию антивирусного программного обеспечения.

Пользователи сети Интернет могут стать жертвами и **преступных посягательств, совершаемых по корыстным мотивам**, при этом возраст потерпевших от подобных действий далеко не всегда старше 18 лет.

Чтобы не стать жертвой подобных преступлений никому и никогда не стоит сообщать подробную информацию о доступной банковской карте, в том числе пин-код, кодовое слово, CVV-код (или CVC2), код 3D-Secure и полученные от банка одноразовые пароли. Если информация о карточке хранится в смартфоне или планшете, не следует переходить по ссылкам, поступившим с неизвестных номеров, а также устанавливать приложения из неизвестных источников. Кроме этого следует помнить, что в том случае если реквизиты карты сохранены в смартфоне или каком-либо аккаунте, то в случае установки платного приложения с изначально

бесплатным пробным периодом, после истечения указанного периода, платная подписка продлится автоматически и денежные средства спишутся со счета.

Занимательные задания по информационной безопасности для детей

Ситуативные задачи. Предложите своему ребенку ответить на вопросы, как бы он поступил, если бы оказался в одной из следующих ситуаций. Проанализируйте полученные ответы вместе. В случаях, когда ребенок затрудняется ответить или предложенный им вариант может привести к отрицательным последствиям, окажите ему помощь и посоветуйте как поступить правильно.

Ситуация 1. Ты общаешься в социальной сети со своими друзьями. Неожиданно от незнакомого тебе человека приходит сообщение: «Привет, у тебя отличные фото! Только у меня все равно круче! Жми скорее сюда!». Предлагается перейти по ссылке для просмотра фотографий. Как следует поступить в данной ситуации?

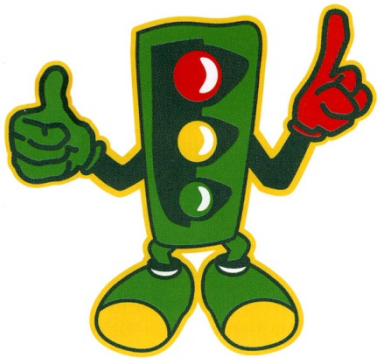
Ситуация 2. Ты находишься в сети Интернет, изучаешь сайты с информацией о далеких планетах. Вдруг наталкиваешься на сайт , который предлагает составить твой личный гороскоп. Ты переходишь по ссылке, отвечаешь на все предложенные вопросы. В конце опроса тебе предлагается ввести номер мобильного телефона. Какими будут твои действия? Почему?

Ситуация 3. Тебе позвонил друг и сообщил, что увидел в Интернет сообщение о срочном сборе средств для больного ребенка. Деньги предлагается перевести на счет указанного мобильного телефона или на электронный кошелек. Твой друг настаивает на помощи ребенку. Какими будут твои действия? Почему?

Ситуация 4. Во время общения в социальной сети тебе приходит сообщение: «Привет! Мы с тобой как-то виделись у наших общих друзей. Решил тебя найти в сетях. Классная у тебя страничка! Может пойдем вечером гулять?» Как ты поступишь в этой ситуации? Почему?

Игра «Светофор»

Предложите детям игру «Светофор». Объясните, что и в сети Интернет должны применяться правила «движения», выполнение которых позволит избежать серьезной опасности для жизни и здоровья. Раздайте каждому участнику карточки зеленого, красного и желтого цветов. Поясните, что красный цвет означает отрицательный ответ, зелёный – положительный, желтый – спрошу совета взрослых. Задавайте участникам вопросы или предлагайте оценить утверждения, используя карточки. Участник, набравший максимальное количество правильных ответов становится инспектором информационной безопасности (ведущим) и продолжает задавать свои вопросы остальным. Игру можно проводить среди отдельных ребят, команд, групп, классов, а также вместе с родителями. Использование таких занимательных форм позволит определить степень усвоения правил работы в Интернете, но и предоставив детям возможность стать ведущими – увидеть уровень осведомленности детей в возможных рисках и угрозах бесконтрольного использования информационных ресурсов.



Предлагаем варианты вопросов и утверждений:

1. Могут ли вредоносные программы украсть вашу переписку с друзьями? (**Да**)
2. Можно ли скачивать игры с неизвестных сайтов? (**Нет**)
3. Можно ли открывать письма от неизвестного вам человека, если он предлагает перейти по определенной ссылке, чтобы посмотреть фотографии, картинки? (**Нет**)
4. Нужно ли советоваться с родителями, если незнакомый человек предлагает совершить какие-либо действия (скачать игру, посмотреть видеоролик)? (**Да**)
5. Все ли сайты в интернете безопасны? (**Нет**)
6. Можно ли использовать сеть Интернет безо всяких опасений? (**Нет**)
7. Может ли общение в социальных сетях принести вам какой-нибудь вред? (**Да**)

Памятка для учащихся:

НИКОГДА:

- Никогда не оставляй встреченным в Интернете людям свой номер телефона, домашний адрес или номер школы;
- Никогда не отправляй никому свою фотографию, не посоветовавшись с родителями;

- Никогда не договаривайся о встрече с интернет-знакомыми без сопровождения взрослых. Они не всегда являются теми, за кого себя выдают. Встречайся только в общественных местах;
- Никогда не открывай прикрепленные к электронному письму файлы, присланные от незнакомого человека. Файлы могут содержать вирусы или другие программы, которые могут повредить всю информацию или программное обеспечение компьютера;
- Никогда не отвечай на недоброжелательные сообщения или на сообщения с предложениями, всегда рассказывай родителям, если получил таковые.

ВСЕГДА:

- 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;
- Всегда спрашивай у родителей разрешения посидеть в чате;
- Всегда покидай чат, если чье-то сообщение вызовет у тебя чувство беспокойства или волнение. Не забудь обсудить это с родителями;
- Всегда держи информацию о пароле при себе, никому его не говори;
- Если ты 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 вы получили оскорбляющие сообщения, расскажите об этом родителям;
- Всегда принимайте помощь от взрослых или друзей, разбирающихся в вопросах безопасного Интернета. Мама и папа могут не знать ответов на все интересующие вас вопросы;
- Всегда помни, что если кто-то сделает тебе предложение, слишком хорошее, чтобы быть правдой, то это, скорее всего, обман;
- Всегда 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.

Материал подготовлен отделом по раскрытию преступлений в сфере высоких технологий УВД Брестского облисполкома