Пути вовлечения несовершеннолетних

в наркобизнес

Обстановка в сфере противодействия незаконному обороту наркотических средств и психотропных веществ на территории Республики Беларусь в настоящее время во многом связана с использованием глобальной сети Интернет в качестве специфического канала наркоторговли.

Особую опасность представляет тот факт, что возможности анонимного приобретения психоактивных веществ с использованием телекоммуникационных устройств в сети доступны широким массам населения. Причины повышенного интереса наркопреступности к киберпространству Интернета вполне понятны: в этой среде есть особые условия не только для обеспечения конспиративной коммуникации поставщиков и потребителей наркотических средств, но и для систематического решения иных масштабных криминальных задач, таких, например, как координация деятельности транснациональных преступных формирований и реализация эффективных схем «отмывания денег».

Широкие возможности анонимного приобретения психоактивных средств с использованием телекоммуникационных устройств в сети, а также участия в сбыте наркотиков получают дети и подростки.

В настоящее время стандартные приемы профилактики становятся малоэффективными, т.к. мы имеем дело со своеобразной молодежной субкультурой, тесно связанной с виртуальным пространством и дистанционным общением. Деятельность и развитие такого интернет сообщества со временем создало благоприятные условия для зарождения некой сетевой среды, где индивиды могут пользоваться средствами общения, вести определенную трудовую деятельность, приобретать и продавать товары и услуги, обучаться, пользоваться развлекательными сервисами.

Этим обстоятельством и пользуются хозяева интернет-магазинов по продаже наркотических средств и психотропных веществ, набирая новых закладчиков и курьеров из числа несовершеннолетних. Они предлагают не только с виду хорошо оплачиваемую работу, не требующую больших физических и временных затрат, но и связанную с использованием привычных гаджетов и Интернета, дающих ложное чувство безопасности и застрахованности от задержания и привлечения к уголовной ответственности.

Соответственно и профилактика должны быть на всех уровнях, не только в виде бесед о недопустимости противоправного поведения, жесткости наказания или вреде употребления наркотиков. Необходимо обращать внимание на ряд вроде бы безобидных признаков, которые свидетельствуют о возможном приближении беды.

Так, первые предложения о трудоустройстве проходят в основном в социальных сетях, как правило это «Вконтакте» и «Одноклассники», либо путем веерной рассылки сообщений о высокооплачиваемой работе в мессенджерах.

После получения согласия дальнейшее общение проходит в одном из мессенджеров, чаще всего в Telegram, здесь же происходит обучение методам конспирации, и основным приемам работы. Также существует система, работающая по принципу финансовой пирамиды, кода за каждого вновь приведенного работника нашедшему полагается денежная премия. В данном случае вербовщиками выступают уже сами дети и подростки.

Таким образом, изначально (это как своеобразная первая линия обороны), необходимо принимать меры к отслеживанию активности несовершеннолетних в сети. С кем они переписываются, что ищут с помощью поисковых систем. Это можно делать как путем непосредственного доступа к телефонному аппарату с ведома ребенка, так установлением одной из программ родительского контроля, большое количество таких приложений совершенно бесплатно и находится в свободном доступе для скачивания.

Дело в том, что большинство используемого наркосбытчиками программного обеспечения имеет специфические функции и не используется рядовыми законопослушными пользователями.

Так наркосбытчики активно используют наборы различных криптографические мессенджеры (VIPole, Telegram, Xabber, Wickr, WeChat, Signal), VPN-сервисы (виртуальные частные сети), анонимные браузеры, выделенные сервера, также ресурсы (фотохостинги, файлообменники) для хранения фотографий с изображениями расположения наркотиков.

В целях сохранения анонимности и скрытости противоправной деятельности стал приобретать популярность анонимный браузер ТOR, «луковый роутер», работающий в теневом сегменте Интернета (DarkNet) и позволяющий пользователям не быть замеченными и уязвимыми. Это система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение. Суть работы данного браузера заключается в том, что он позволяет гражданам посещать сайты, заблокированные на территории страны проживания, путем замены IP адреса, оставаясь при этом незамеченными.

Даркнет - это самый закрытый отдел мировой паутины (своеобразная, глубинная, не видная обычному глазу часть айсберга, причем как и в случае с айсбергом гораздо более массивная), куда не заходят даже поисковые роботы. Обычный интернет-пользователь тоже вряд ли попадет сюда случайно, хотя тот, кому сюда по-настоящему нужно, попадет, куда ему необходимо без особого труда. Чем больше развивается интернет-цензура, тем более даркнет становится востребованным и тем более удобными становятся инструменты для работы с ним. И если во всем остальном интернете владельцы сайтов пытаются повысить рейтинг сайта и увеличить его посещаемость, то вот в темном сегменте стараются сделать сайт как можно менее заметным для рядовых сторонних пользователей, и, естественно, для органов правопорядка. Для этого используется шифрование, специальное программное обеспечение, а также нестандартные доменные имена и протоколы (смотри слайд). Так вот, для того чтобы попасть в даркнет, необходимо использовать браузер ТOR. Это своеобразный теневой аналог используемых всеми стандартных браузеров операционной системы и поисковиков. Ключевой момент здесь состоит в том, что при его использовании резко теряется скорость интернет-соединения, это обусловлено его техническими особенностями функционирования. Поэтому в обычной повседневной деятельности он и не используется, а применяется только для выхода в даркнет и соблюдения мер конспирации. Нахождение подобной программы на компьютере или телефоне ребенка прямой сигнал о том, что он уже втянут во что-то противозаконное или это вот-вот случится.

Итак, технология ТОР позволяет заходить на сайты и скачивать что-то из сети **не оставляя после себя никаких следов.**

Это же относится к использованию для подключения к различным интернет-ресурсам прокси-серверов это (комплекс программ) в [компьютерных сетях](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C), позволяющий [клиентам](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B8%D0%B5%D0%BD%D1%82_%28%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0%29) выполнять косвенные запросы к другим сетевым службам, и VPN ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) Virtual Private Network – виртуальная частная сеть) – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, [Интернет](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82)). Данные приложения позволяют обходить запреты на посещение определенных сайтов. Например, нами постоянно ведется работа по отслеживанию сайтов пронаркотической направленности и блокировке доступа к ним с территории Республики Беларусь. А при помощи VPN или прокси данная блокировка удачно обходится.

Повторюсь, в обычной жизни вышеуказанные приложения (за исключением мессенджеров Viber и Telegram) как правило гражданами не используются. Они достаточно специфические и основная их цель – скрыть свое истинное местонахождение в сети.

Если у ребенка вдруг в телефоне появились приложения, позволяющие определять GPS-координаты и накладывать их на фотографии (например, NoteCam или его аналоги), стоит уделить этому пристальное внимание, т.к. данное программное обеспечение на 90% используется исключительно сбытчиками наркотиков. Согласитесь, что никто в обычной жизни не будет накладывать координаты с указанием широты, долготы, высоты над уровнем моря и погрешности на фотографию понравившегося пейзажа или живописного дерева.

Итак, как уже было сказано, использование программ для посещения даркнета, набора мессенджеров, особенно содержащих чаты в закрытых группах, приложений для определения GPS-координат, специального обеспечения для скрытия истинных IP-адресов совершенно не нужно для обычного общения и эксплуатации смартфонов или персональных компьютеров. Их появление свидетельствует о вовлечении ребенка в противоправную деятельность.

Что касается обычного сайта наркоторговцев, то он выглядит как классический форум. Много веток, содержащих разнообразный контент, с возможностью комментариев и вывод удачных высказываний в отдельную ветку.

Теперь перейдем к главной составляющей любой работы, легальной или нет. Собственно говоря, это ее оплата.

В настоящее время использование электронных кошельков при организации сбыта наркотиков становится менее актуальным в связи с тем, что финансовая составляющая наркобизнеса в основном переориентировалась на криптовалюту, которая не имеет физического выражения, ее эмиссию никто не регулирует и не контролирует. Криптовалюта выпускается непосредственно в сети и никак не связана ни с какой-либо обычной валютой, ни с любой государственной валютной системой. Все операции с криптовалютой фактически обезличены. Но, образно говоря, сладостей за криптовалюту не купишь, ее надо менять, а это тоже делается в виртуальном пространстве. Отсюда возникает необходимость в банковских картах.

Также отдельными крупными магазинами для выплаты заработной платы в настоящее время используются обычные банковские платежные карты, в том числе и оформленные на имя учащихся карты ОАО «АСБ Беларусбанк». Однако, наркодилерами могут выдаваться закладчикам и карты¸ оформленные на подставных лиц, в том числе и иностранных банков (как правило российских).

Также необходимо обращать внимание на попытки регистрации на криптообменных площадках, использовании электронных денег, неизвестных Вам сим-карт, банковских платежных карт и т.д.

ГУНиПТЛ КМ МВД Республики Беларусь