Разъяснения о формах и методах втягивания российских граждан, в том числе посредством телефонного мошенничества, компьютерных игр, иных технологий, использующих возможности искусственного интеллекта, в диверсионно-террористическую деятельность

В настоящее время развернулась тихая, но коварная работа по вербовке россиян и добыче разведданных в сети Telegram.

С украинской стороны сейчас делается большая ставка на внутреннюю дестабилизацию России и теракты на нашей территории, в связи, с чем схемы вовлечения российских граждан в противоправную деятельность достаточно изощрены.

Схема деятельности врага, следующая: сотрудники украинских спецслужб создают в сети Telegram каналы, которые занимаются сбором данных из открытых источников. Пользователи вовлекаются в игровые задания, под прикрытием которых ведётся сбор разведданных и вербовка пользователей.

Пользователь отвечает вроде бы на обычные вопросы и незаметно для себя раскрывает личную информацию. Дальше к работе подключаются психологи, которые, основываясь на полученной информации, уже начинают вербовать человека. Чаще всего такой сбор информации маскируется под обычные квесты, когда пользователям предлагается зайти на какие-то ресурсы, найти определённую информацию, отгадать загадки и собрать ключи и т.д. Игровой формат сбивает пользователей с толку, они думают, что это безобидно, и даже не перепроверяют полученную информацию.

Ещё один распространённый метод разведки и вербовки молодёжи вражескими спецслужбами — так называемые игры ARG (Alternative Reality Games). В них задания тоже даются в интернете, а вот игровой платформой становится реальный мир. Несмотря на то, что всё происходящее преподносится как игра, в ней используются реальные номера телефонов, локации, даже вознаграждение победителю. Поначалу игрокам даются простые и как будто безобидные здания — например, сфотографироваться рядом с определённым зданием в городе или объектом оборонного комплекса и передать снимок организаторам. По сути же, так участник неосознанно совершает преступление. После этого манипулировать им можно с помощью угроз и шантажа, а задания становятся, по сути, диверсиями.

Неспроста площадкой для своей деятельности иностранные спецслужбы выбрали Telegram. За годы существования сети у неё сложилась репутация надёжного ресурса с системой шифрования и верификацией каналов. В итоге у людей складывается ложное ощущение безопасности.

Вместе с тем наиболее уязвимая категория пользователей, на которых делают ставку спецслужбы, — это подростки. С учётом их интересов легко войти к ним в доверие и воспользоваться гибкостью подростковой психики. Сегодня для этого даже не нужно лично встречаться, как в классических фильмах про шпионов, достаточно создать телеграм-канал с привлекательным для подростков контентом. Главное правило и защита от подобных манипуляций в интернете — перепроверка достоверности любой получаемой информации. Например, можно поискать информацию о каком-то описываемом в телеграм-канале мероприятии на официальном сайте организатора — действительно ли он проводит ту или иную игру, квест, конкурс и т.д.

Виды информационно-психологического влияния

1. Создание информационных ресурсов, замаскированных под местные ресурсы и/или закупка существующих местных информационных ресурсов.
2. Создание игровых информационных ресурсов, которые будут проводить городские квесты и т.п. Например, каналов, групп в социальных сетях, веб-сайтов и т.п. Любые информационные ресурсы, которые ориентированы на местных жителей региона, либо на определённую социальную группу.
3. Размещение на популярных сайтах, видеохостингах и иных сервисах в качестве рекламы в текстовой, фото или видео форме материалов о потерях личного состава и военной техники РФ, зачастую с демонстрацией убитых солдат.
4. Телефонный терроризм:

— рассылка SMS сообщений с угрозами, недостоверной информацией;

— телефонные звонки с анонимных номеров с угрозами;

— телефонные звонки с целью шантажа и/или предложением выкупа пленных военнослужащих, а также родственников, захваченных спецслужбами Украины;

— телефонные звонки с ложными сообщениями о гибели их близких родственников в зоне СВО с целью оказания психологического давления;

5. Публичное распространение или угроза распространения персональных данных как военнослужащих, так и гражданских лиц, активно выражающих свою патриотическую позицию. Эти акции проводится с целью устрашения, склонения к сотрудничеству или втягиванию в другую незаконную деятельность. Их необходимо игнорировать. Помните, что любое взаимодействие с противником — незаконно.
6. Создание и популяризация различных якобы гуманитарных программ.
7. Создание и популяризация экстремистских организаций псевдопатриотического толка в сети Интернет. Реализуется через рекламу, рассылку сообщений, создание и распространение медиаконтента.
8. Сообщения в сети Интернет о действиях т.н. «украинского подполья» на подконтрольных РФ территориях (фотографии размещения листовок проукраинского содержания, размещение лент в цветах украинского флага, фотографии граффити проукраинского или экстремистского содержания на стенах зданий и т.п.; зачастую являются подложными — фото, видеомонтаж, подмена локации).
9. Операции спецслужб противника, направленные на вовлечение молодежи в незаконную деятельность. Например: в сети «Интернет» создаётся и рекламируется информационный ресурс, который проводит городские игры, квесты и т.п. К примеру, по принципу игры в альтернативной реальности, интерактивное повествование с игровыми элементами, использующие в качестве платформы реальный мир.
10. Отправка жене или другому члену семьи участника СВО фотографий школы, где учится ребёнок, либо фотографии дома, входной двери квартиры, где проживает семья или любых других подобных фото/видео материалов. Материалы якобы являются доказательством того, что «диверсанты» нашли семью военнослужащего и обычно сопровождаются угрозами совершения противоправных действий в отношении близких/ родственников, в случае если он откажется дезертировать или сдаться в плен.
11. Создание и популяризация информационных ресурсов и блогеров якобы из числа местных жителей.

12. Создание сайтов и телеграмм-ботов для сбора информации о военнослужащих РФ от имени спецслужб Украины с призывом к проукраинской общественности. Возможен вариант маскировки под российские государственные и общественные ресурсы (например, сайты мемориалы ветеранов СВО, фейковые телеграмм-боты армии ДНР или иных подразделений, сайты оказания помощи военнослужащим СВО и их семьям или юридических консультаций незаконно мобилизованным).
13. Создание и распространение фейковых материалов о военных преступлениях и других противоправных действий со стороны военнослужащих:
— о бытовых преступлениях в виде мародерства и хищений собственности мирных жителей;
— о военных преступлениях;
— заявления официальных лиц Украины с недостоверной информацией о якобы изнасиловании несовершеннолетних граждан российскими военнослужащими или других военных преступлениях;
— обвинения в жестоких пытках над украинскими военнопленными и гражданскими лицами Украины;
— применение «языка ненависти» — распространение в украинских СМИ уничижительных прозвищ в отношении граждан РФ и людей русской национальности «ватники», «колорады», «личинки колорадов», «самки колорадов», «русня», «орки», «гоблины», «обезьяны», «недочеловеки» ит.д.; — распространение публикаций и заявлений о якобы трусости российских военнослужащих и их нежелании воевать (прежде всего, из числа мобилизованных лиц), а также о якобы паническом бегстве подразделений ВС РФ в случае малейшего наступления ВСУ.
14. Подложные сообщения от очевидцев про обстрелы населенных пунктов со стороны ВСРФ.
15. Распространение публикаций, в которых высказывается мнение, что резонансные убийства и покушения на территории РФ организованы российскими спецслужбами.
16. Распространение фейковых материалов о больших потерях ВС РФ и огромном количестве пленных.
17. Публикация и распространение кадров с убийством пленных россиян или раненных российских солдат на поле боя, а также демонстративное изувечивание тел погибших солдат РФ.
18. Распространение фейковых рейтингов и искаженной статистики о социальных процессах, общественно значимых событиях или политических лидерах.
19. Телефонное мошенничество. Звонки гражданам России. Злоумышленники могут представляться сотрудниками банка, полиции, пенсионного фонда, ЖЭКа и т.п. Задача подобных акций — получение личных данных вас или ваших родственников, информации о ваших счетах и банковских картах. В худшем случае — подстрекательство к совершению незаконной деятельности (теракты, поджоги, нанесение телесных повреждений третьим лицам и т.п.). Например, поджог машины, здания военкомата или районного отдела полиции. Предлогом может послужить уничтожение имущества жертвы, чтобы при оформлении этого происшествия, полиция установила владельца авто и обнаружила, что он в розыске и т.п.
20. Распространение недостоверной информации о полной мобилизации в РФ.
21. Призывы к организации незаконных митингов, собраний и протестов с целью дискредитации СВО.
22. Подстрекание близких родственников участников СВО организовать митинг или обратиться в СМИ с заявлениями о бедственном положении мужей и сыновей в зоне СВО.
23. Новостные материалы о регулярных визитах западных политиков на Украину и ответных визитах украинских политиков в западные страны.
24. Сотрудники украинских спецслужб создают страницы на информационных ресурсах предназначенных для знакомств под видом красивых девушек.
25. Постановочные видео (фейки).
Здесь перечислены лишь некоторые методы информационно-психологического влияния. Однако теперь, вы точно сможете распознавать как перечисленные, так и любые другие методы такого влияния. Помните, что всегда нужно сохранять критическое мышление. Ищите

логику и здравый смысл в получаемой информации. Любые информационные материалы, в каком бы виде они не подавались, направлены лишь на то, чтобы получить от вас информацию, спровоцировать вас на совершение ошибок, побудить к благоприятным для оппонента действиям, а главное — всегда на причинение вреда вам, вашим близким и вашей стране.

Ответственность за совершенные противоправные действия:

(Уголовный Кодекс Российской Федерации)

Статья 205. Террористический акт. Предусмотрено лишение свободы на срок от десяти до двадцати лет, в некоторых случаях наказывается пожизненным лишением свободы.

Примечание. Лицо, участвовавшее в подготовке террористического акта, освобождается от уголовной ответственности, если оно своевременным предупреждением органов власти или иным способом способствовало предотвращению осуществления террористического акта и, если в действиях этого лица не содержится иного состава преступления.

Статья 205.1. Содействие террористической деятельности. Предусмотрено лишение свободы на срок от восьми до двадцати лет, в некоторых случаях наказывается пожизненным лишением свободы.

Примечания.

1. Под финансированием терроризма понимается предоставление или сбор средств либо оказание финансовых услуг с осознанием того, что они предназначены для финансирования организации, подготовки или совершения хотя бы одного из преступлений терроризма, либо для финансирования или иного материального обеспечения лица в целях совершения им хотя бы одного из этих преступлений, либо для обеспечения организованной группы, незаконного вооруженного формирования, преступного сообщества.
2. Под пособничеством терроризму понимаются умышленное содействие совершению преступления советами, указаниями, предоставлением информации, средств или орудий совершения преступления либо устранением препятствий к его совершению, а также обещание скрыть преступника, средства или орудия совершения преступления, следы преступления либо предметы, добытые преступным путем, а равно обещание приобрести или сбыть такие предметы.
3. Лицо, совершившее преступление, предусмотренное настоящей статьей, освобождается от уголовной ответственности, если оно своевременным сообщением органам власти или иным образом способствовало предотвращению либо пресечению преступления, которое оно финансировало и (или) совершению которого содействовало, и если в его действиях не содержится иного состава преступления.