МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ
для проведения информационно-разъяснительной работы с персоналом предприятий и организаций военно-промышленного комплекса.

Зарубежные спецслужбы плотно освоили метод дистанционного вовлечения граждан в совершение диверсионно-террористических преступлений, как в формате непосредственно диверсионно-террористических актов (ДТА), так и в формате содействия (материального, информационного и иного) террористическим структурам.

Работники предприятий и организаций военно-промышленного комплекса, иных критически важных предприятий и организаций, в силу исполняемых функций, представляют для структур, планирующих ДТА, особый интерес. Необходимо помнить, что ряд предприятий, помимо того, что представляют стратегическую ценность, сами по себе являются источником повышенной опасности (например, в силу наличия радиоактивных, отравляющих, взрывчатых веществ) или выступают знаковым звеном в цепочке процессов жизнеобеспечения населения). Совершение диверсии на подобном объекте не только способно вывести его из строя и нанести экономический ущерб, но и способно представлять серьезную угрозу безопасности гражданам.

В этой связи, помимо стандартных для других граждан форм совершения ДТА, работники рассматриваемых предприятий и организаций (в зависимости от исполняемых функций, уровня допуска, квалификации) могут склоняться к совершению специфических акций, например, посредством выведения из строя оборудования или иных объектов, способного спровоцировать техногенные аварии, привести к дестабилизации работы предприятия и (или) целой технологической (функциональной) цепочки. Работники особо важных предприятий также представляют для противника интерес в качестве источников информации, пособников диверсионных операций.

Данные обстоятельства налагают особую ответственность на службы безопасности предприятий и организаций военно-промышленного комплекса.

В текущих условиях следует уделять повышенное внимание мерам безопасности на объектах, включая:

- соблюдение контрольно-пропускного режима, исключающего не только проникновение на объект посторонних лиц, но и штатных работников, пребывание которых на объекте не соответствует их расписанию работы;

- соблюдение внутреннего порядка, исключающего свободное перемещение работников по объекту, не обусловленное исполняемыми функциями, бесконтрольное перемещение и (или) оставление без наблюдения работников сторонних организаций, выполняющих на территории предприятия (организации) те или иные виды работ;

- соблюдение информационной безопасности, исключающее распространение сведений служебного характера (даже не имеющих статуса сведений, содержащих государственную и иную охраняемую законом тайну) среди лиц, не имеющих, в силу

исполняемых функций, необходимости в ознакомлении с ними.

Также на руководство и иных ответственных за данное направление работников ложится обязанность по проведению индивидуальной и массовой информационно-разъяснительной работы с персоналом предприятий (организаций) в целях противодействия деятельности противника по вовлечению граждан в диверсионно-террористическую деятельность.

Практика показывает, что противник применяет широкий спектр вербовочных методов, включая их комбинации. Основными механизмами выступают:

1) Идеологическое воздействие.

Работникам, особенно интересующимся социально-политической проблематикой и посещающим информационно-коммуникационные ресурсы оппозиционного характера, могут внушаться мысли об их причастности к «военным преступлениям» и обязанности «искупить вину» оказанием помощи, допустим, противникам специальной военной операции.

Не исключены варианты с подкреплением идеологической обработки конкретными предложениями материального характера (например, предоставление вида на жительство в иностранном государстве и подъемных средств).

Массовая разъяснительная работа в отношении подвергшихся указанному воздействию лиц обычно не демонстрирует должную эффективность, поэтому, при выявлении работника, имеющего подобные проблемы, целесообразно провести с ним индивидуальные беседы, направленные на нейтрализацию пропагандистского воздействия.

Кроме того, в профилактических целях рекомендовано поддерживать соблюдение работниками мер личной информационной безопасности, не позволяющих идентифицировать их в качестве работников предприятий и организаций военно-промышленного комплекса (и, как следствие, представляющих особый интерес для вербовщиков), а также препятствующих сбору компромата в целях шантажа. Необходимо разъяснить работникам важность данных мер, поскольку в качестве материала для шантажа часто выступают сведения, публикуемые самими жертвами, причем шантажисты искусно создают необходимые условия, например, провоцируя дискуссии в сети Интернет в целях задокументировать определенные высказывания, вступая в романтические знакомства с последующим обменом фотографиями личного характера и тому подобными способами.

2) Найм.

Основной платформой для поиска жертв выступают сайты и сообщества для поиска работы, вакансий, где вербовщики могут размещать объявления с предложением быстрого и крупного заработка, могут и сами направлять лицам, выступающим соискателями трудоустройства, предложения о «разовой подработке».

Основные признаки криминальных предложений:

- обещание легкого и быстрого заработка;

- разовые выплаты за разовую работу;

- гарантии анонимности;

- широкий спектр возможных выплат (от безналичных переводов до переводов в криптовалюте).

Вербовщиков может интересовать не только непосредственное исполнение ДТА, но и исполнение иных действий, например:

- осуществить перевозку каких-либо предметов, оборудование мест их скрытого хранения, осуществить перевозку сторонних людей;

- провести разведывательные мероприятий (сбор информации, фотосъемка, видеозапись и т.п.);

- предоставить во временное пользование третьих лиц свои аккаунты, иные учетные записи в сети Интернет, телефоны, банковские или криптовалютные счета, совершить какие-либо операции (например, перевести на иной счет полученные денежные средства, обналичить денежные средства, приобрести, перевести или обналичить криптовалюту и т.п.), а также отдельно зарегистрировать что-либо из перечисленного на свое имя с последующей передачей иным лицам.

Иногда предложения о найме могут поступать не напрямую, а через третьих лиц, выступающих посредниками (данный механизм обязательно нужно учитывать, так как предложение, поступающее при очном контакте, вызывает больше доверия и может не рассматриваться человеком столь же опасным, как полученное через Интернет).

Также необходимо иметь в виду, что вербовщиками используются легенды. Зафиксированы факты вовлечения граждан в совершение ДТА под предлогом участия в проверках работы нарядов МЧС или, например, работоспособности систем сигнализации. В этой связи работникам нужно четко донести недопустимость приема подобных предложений.

3) Психологическая обработка.

Данный способ требует особого внимания, так как, во-первых, используется достаточно массово, во-вторых, практика убедительно показывает уязвимость к нему людей обоих полов, всех возрастных групп, уровня образования и иных категорий.

Из этого следует, что ни должность, ни стаж работы на предприятии не являются гарантией от возможности вовлечения работника в диверсионно-террористическую деятельность.

Основные формы манипуляций: обман, шантаж, угрозы.

Как правило, вербовщики используют стандартный алгоритм:

1. На человека выходит вербовщик (иногда работают группой, сменяя друг друга), представляясь сотрудником правоохранительных органов и специальных служб России, и сообщает ему, что он нарушил закон (обычно вербовщики оперируют особо тяжкими составами, наподобие статьи 275 УК РФ «Государственная измена», статьи 205.1 УК РФ «Содействие террористической

деятельности» и т.п.).

Поводы для такого контакта, как правило, предварительно создаются самими вербовщиками и могут быть различными.

Одним из сценариев выступает мошенническое хищение денежных средств жертвы с последующим обвинением ее же в финансировании вооруженных сил противника или террористических организаций. Тут работникам стоит отдельно разъяснить беспочвенность таких обвинений, так как ответственность гражданина за использование злоумышленниками похищенного у него имущества российским законодательством не предусмотрена.

Вторым распространенным сценарием выступает знакомство в сети Интернет (как правило, через сайты или группы знакомств), непродолжительная переписка, скинутая геолокация или фотографии, после чего жертву обвиняют в «разглашении государственной тайны», «выдаче врагу секретных сведений» и т.п. (что тоже, надо отмечать, является пустой уловкой, не имеющей под собой оснований)

Для взрослых и семейных сотрудников возможны варианты с Интернет-романом, сам факт которого станет предметом шантажа. Возможно, первоначальные требования будут не особо серьезными (например, нанести на здание пропагандистскую надпись или предоставить какую-нибудь информацию), но их исполнение, в свою очередь, послужит новым и более значимым компроматом.

Часто, для пущего эффекта, предварительно жертве приходит видеозапись, где, например, человек в военной форме с украинской символикой благодарит его за помощь и обещает, что предоставленные им сведения послужат на благо Украины. После такого сообщения звонок «сотрудника ФСБ» оказывается более убедителен.

2. Человека стараются оградить от возможных контактов, способных расстроить схему вербовки: его предупреждают о секретности всех переговоров и «ответственность за разглашение государственной тайны». Известны случаи написание жертвами под диктовку вербовщика письменного обязательства сотрудничать с «органами безопасности» и предупреждения об ответственности за разглашение. Такие «документы» юридической силы не имеют, но факт их написания на жертву оказывает дополнительное воздействие.

3. Подвергшемуся обработке человеку дают поручение на выполнение каких-либо действий, чаще всего – ДТА (хотя, как и в случае с наймом, не исключены поручения иного характера, для работника предприятия оборонно-промышленного комплекса такими вполне могут стать разведывательные мероприятия или иное содействие диверсантам).

4. Исполнение поручения сопровождается фото- и видеофиксацией своих действий (для ДТА иногда используется трансляция в прямом эфире). Подтверждением исполнения поручения на разведывательные мероприятия служат отправляемые сведения.

5. После исполнения поручения обычно контакт прерывается, сообщения часто удаляются, жертва вербовки оказывается один на один со своими проблемами. В редких случаях успешного выполнения поручения (например, в виде предоставления какой-либо интересовавшей вербовщика информации) могут последовать новые задания, причем факт исполнения предыдущих послужит дополнительным рычагом воздействия.

Слабым местом механизмов найма и психологической обработки выступает отсутствие идейной вовлеченности жертвы в интересы вербовщика, вследствие чего осведомленность граждан об опасности данного рода процессов, неизбежности наказания, несоотносимости возможных выгод (в случае найма) и ущерба собственной жизни (в виде длительного срока заключения), а главное – о методах действия вербовщиков, может послужить достаточно эффективным способом противодействия.

Важно регулярно закреплять и актуализировать (с учетом новых форм и способов вербовок) вышеизложенную информацию в сознании людей как посредством наглядных информационных материалов, так и информационно-разъяснительных занятий.

Подготовлено Центром «Э» ГУ МВД России по г. Санкт-Петербургу и Ленинградской области