УДК 343.985.8

А.В. Балиткин

ИСПОЛЬЗОВАНИЕ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ ПРИ ДЕАНОНИМИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ МЕССЕНДЖЕРОВ С ЦЕЛЬЮ РЕШЕНИЯ ЗАДАЧ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Анализ современного состояния правоприменительной практики позволяет выявить тренд роста использования информационно-коммуникационных технологий в преступной деятельности. Сервисы мгновенного обмена сообщениями со встроенными алгоритмами шифрования обосновались в списках используемого злоумышленниками программного обеспечения по ряду причин, основными из которых являются: повсеместность использования, возможность взаимного удаления данных, условная анонимность пользователей (в том числе сложность их деанонимизации).

Действительно, в современных условиях динамично развивающегося информационного поля, используемого преступниками для разработки новых методов анонимизации и противодействия правоохранительным органам, их идентификация усложняется, а получение оперативной информации о личности злоумышленников становится важной проблемой, требующей разработки научных рекомендаций в виде универсальных тактических приемов.

Одним из инновационных способов решения данной проблемы, должным образом не освещенным в научной литературе по отношению к другим, может выступать использование методов социальной инженерии, оперирующей понятием «социо-психологические манипуляции», которые применяются (в том числе преступниками) для получения доступа к защищенным компьютерным системам (включая мобильные устройства) с целью получения интересующей информации.

Обзор публикаций и тематических форумов в сети Интернет свидетельствует, что аналогичный термин присутствует в профессиональном сленге сотрудников правоохранительных органов – специалистов в сфере обеспечения информационной безопасности и встречается в научных исследованиях. Наиболее полно сущность данного термина, в том числе применительно к правоохранительной деятельности, в своих трудах рассматривает М.В. Губич, а его позиция использована нами в качестве основы для разработки научных рекомендаций, конечным результатом которых должно выступить решение определенных задач оперативно-розыскной деятельности (ОРД).

В зависимости от конкретно сложившейся ситуации, тактика и последовательность действий оперативных сотрудников будет различной, в связи с чем представить их исчерпывающий перечень в данной пубикации не представляется возможным. Вместе с тем в целях полноты исследования можно выделить основные приемы получения информации об интересующем лице (деанонимизации), отразив кратко их сущность.

Первый прием, используемый оперативным сотрудником, направлен на введение интересующего лица в заблуждение и понуждение к выполнению необходимых для его деанонимизации (идентификации) действий.

Второй прием также характеризуется активностью оперативного сотрудника, однако она направлена на создание для интересующего лица таких обстоятельств (или их видимости), при которых он инициативно выполняет действия в интересах оперативного подразделения, не подозревая об этом.

Таким образом, использование методов социальной инженерии при деанонимизации пользователей мессенджеров в целях решения задач ОРД представляется перспективным направлением для научных исследований, широкое изложение результатов которого возможно в специализированных научных изданиях ввиду ограниченного распространения таких сведений.

УДК 004

П.Л. Боровик

НЕФОРМАЛЬНАЯ МОДЕЛЬ ВОЗМОЖНОГО ПРАВОНАРУШИТЕЛЯ В КОНТЕКСТЕ МОДЕРНИЗАЦИИ ВЕДОМСТВЕННОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В настоящее время в органах внутренних дел (ОВД) проводится последовательная работа по модернизации ведомственной системы информационной безопасности (ИБ), основывающаяся на качественно новых подходах. Так, приказом Министерства внутренних дел Республики Беларусь от 30 сентября 2022 г. № 256 «О единой цифровой платформе Министерства внутренних дел» утверждены входящие в состав документированной информации в области обеспечения ИБ нормативно-методические документы, направленные: на определение парольной политики и организации порядка доступа к отдельным сегментам ведомственной сети передачи данных (ВСПД) ОВД; защиту от вредоносного программного обеспечения; криптографическую защиту информации; межсетевое экранирование периметра ВСПД ОВД; мониторинг, аудит событий ИБ и оперативное реагирование на инциденты безопасности; организацию резервного копирования информации и др.

В контексте широкого спектра рисков и угроз национальной безопасности в информационной сфере, обозначенного в Концепции национальной безопасности Республики Беларусь (утвержденной Указом Президента Республики Беларусь от

9 ноября 2010 г. № 575) такое решение представляется крайне актуальным и востребованным, поскольку предполагает крайне необходимый сегодня комплексный подход к нейтрализации либо эффективной минимизации соответствующих негативных проявлений и тенденций с учетом весьма весомого пакета ведомственной специфики.

Наряду с предпринимаемыми организационно-правовыми мерами обеспечения ведомственной ИБ дополнительной гарантией построения эффективной системы ее обеспечения может стать разработка неформальной научно-обоснованной модели возможного правонарушителя – набора предположений об одном или нескольких возможных нарушителях ИБ, их мотивации, квалификации, используемых ими программных и технических средствах. Данное утверждение аргументируется тем, что наиболее уязвимым звеном любой системы обеспечения ИБ является, как известно, человек. В рассматриваемом контексте он не только имеет прямой либо косвенный доступ к защищаемой информационной системе (ИС), но и подвержен различным проявлениям человеческой слабости (усталость, забывчивость, корысть, продажность, слабохарактерность и др.), в том числе методам социальной инженерии со стороны вероятного противника. При определенных условиях такое лицо может стать правонарушителем, предприняв попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради любопытства, с целью самоутверждения и т. п.) и используя для этого различные возможности, методы и средства.

Результаты анализа эмпирических данных, полученных в ходе изучения инцидентов ИБ, описанных в специальной литературе, а также материалов оперативно-следственной и судебной практики по делам о преступлениях против компьютерной безопасности за последние несколько лет позволяют выдвинуть предположение о существовании двух основных видов нарушителей ИБ: внутреннего и внешнего (по отношению к защищаемой ИС).

Внутренний нарушитель представляет собой зарегистрированного пользователя ИС, который действует сознательно из личных интересов или с целью мести за причиненный ущерб. Такой нарушитель может применять разнообразные методы и средства для преодоления системы защиты информации (СЗИ), включая агентурные методы для получения учетных данных, использование пассивных средств (технические устройства для перехвата без модификации компонентов системы), а также активные методы и средства воздействия (модификация технических устройств, подключение к каналам передачи данных, внедрение вредоносного программного обеспечения и использование специализированных программ и аппаратных средств). При этом он может комбинировать воздействия как изнутри, так и извне – через сети общего пользования.

Внутренним нарушителем может быть лицо из следующих категорий пользователей ИС: зарегистрированные пользователи ИС; работники, не допущенные к работе с ИС; персонал, обслуживающий технические средства ИС (инженеры, техники); работники подразделений разработки и сопровождения ПО (прикладные и системные программисты); технический персонал, обслуживающий здания (уборщицы, электрики, сантехники и другие работники, имеющие доступ в здания и помещения, где расположены компоненты ИС); работники и подразделения ИБ; руководители различных уровней.

Внешний нарушитель – постороннее лицо или зарегистрированный пользователь ИС, который действует целенаправленно по собственным корыстным мотивам, из мести или из любопытства, возможно, в сговоре с другими лицами. Ему доступен полный спектр радиоэлектронных методов нарушения ИБ, а также методы и средства преодоления СЗИ, характерные для сетей общего пользования (удаленное внедрение вредоносного программного обеспечения, использование специального программно-аппаратного обеспечения и др.).

Категории лиц, которые могут быть внешними нарушителями: уволенные сотрудники ОВД; представители организаций, сотрудничающих по вопросам обеспечения жизнедеятельности подразделения ОВД, включая энергоснабжение, водоснабжение, теплоснабжение и пр.; посетители (приглашенные граждане, представители организаций, поставляющих технику, программное обеспечение, различные услуги и т. п.); члены преступных организаций, работники спецслужб или лица, действующие по их заданию; лица, случайно или умышленно проникшие в ведомственную сеть из внешних сетей.

Сотрудники ОВД и гражданский персонал, включая пользователей ИС, обладают широкими возможностями для совершения неправомерных действий из-за наличия определенных полномочий по доступу к ресурсам ИС и глубокого понимания технологий обработки информации и СЗИ. Действия этой группы прямо связаны с нарушением установленных правил и инструкций. Особую опасность представляет их сотрудничество с преступными структурами или иностранными спецслужбами.

Бывшие сотрудники ОВД имеют возможность применять свои знания о технологии работы, СЗИ и правах доступа для достижения своих целей. Опыт и навыки, полученные в подразделениях ОВД, выделяют их среди других потенциальных внешних угроз.

Для построения модели возможного правонарушителя используется информация, полученная от служб и подразделений ИБ, технической защиты информации и аналитических групп, а также сведения о существующих средствах доступа к информации и ее обработке. Рассматриваются возможные методы перехвата данных на этапах их передачи, обработки и хранения, анализируется обстановка в коллективе и на объекте защиты, случаи нарушения ИБ и др. Проводится оценка фактических технических возможностей потенциального злоумышленника для воздействия на СЗИ или защищаемый объект.

Таким образом, при создании либо модернизации ведомственной СЗИ ИС мы рекомендуем разрабатывать и применять в повседневной деятельности ОВД неформальную модель возможного правонарушителя ИБ, построенную на основе эмпирических данных, учитывающих предположения о его видах, мотивах, квалификации, наличия у него специальных технических средств, а также иных смежных и сопутствующих качеств. Это позволит получить более четкое представление о существующих рисках и угрозах ИБ, разработать на их основе эффективную систему мониторинга и обнаружения инцидентов; повысить качество и оперативность реагирования на подозрительную активность, в том числе принятия своевременных мер для предотвращения (нейтрализации) угрозы; обеспечить более высокий уровень ведомственной информационной безопасности в целом.