операции. Замысел является системообразующим фактором, формирующим оперативно-тактическую операцию. Проработка замысла предполагает определение пространственно-временных границ проведения оперативно-тактической операции и согласование в этих рамках порядка и тактики проведения ОРМ и иных мероприятий. В этом смысле согласование времени проведения мероприятий в рамках операции предполагает установление временного промежутка, в ходе которого они будут осуществляться в определенной последовательности, а места – выбор участка местности, на котором они будут вестись.

Во-вторых, субъектами оперативно-тактической операции являются сотрудники уполномоченных оперативных подразделений.

Законом об ОРД в ч. 5 ст. 19 установлено, что ОРМ подготавливается и проводится должностным лицом оперативно-розыскного органа. В соответствии с абз. 20 ч. 1 ст. 14 оперативно-розыскные органы определяют подразделения и должностных лиц, которые наделяются правом осуществлять ОРД. При этом не все уполномоченные подразделения вправе вести ДОУ. Таким образом, субъектами рассматриваемой операции будет являться сотрудник уполномоченного оперативного подразделения, который вправе вести ДОУ.

В-третьих, целью проведения оперативно-тактической операции является решение сложной тактической задачи в рамках ДОУ.

Потребность проведения ОРМ, иных действий, а также принятия соответствующих решений обусловлена необходимостью решения сложной тактической задачи, которая: появляется как неизбежный и единственный логический результат работы оперативного сотрудника по ДОУ; требует использования как оперативно-розыскных, так и иных возможностей (управленческих, административно-процессуальных, уголовно-процессуальных, технических и иных) для своего разрешения; обеспечивает безусловное достижение целей ведения ДОУ (в первую очередь пресечение преступной деятельности).

С учетом этого могут быть выделены следующие основные сложные тактические задачи, которые могут быть решены посредством проведения оперативно-тактической операции: захват объекта ДОУ с поличным; компрометация объекта ДОУ перед окружением; разобщение преступной группы; пресечение или дискредитация канала преступной деятельности через Государственную границу Республики Беларусь.

Таким образом, основываясь на выделенных существенных признаках оперативно-тактическая операция может быть определена как система ОРМ и иных мероприятий, проводимых сотрудниками уполномоченных оперативных подразделений оперативно-розыскных органов по ДОУ, а также принимаемых ими в связи с этим решений, объединенных единым замыслом и взаимосвязанных по месту и времени, целью которых является решение сложной тактической задачи в рамках ДОУ.

Здесь необходимо отметить, что рассматриваемые оперативно-тактические операции отличаются от тактических операций в криминалистике тем, что проводятся в ходе ОРД (а не в процессе предварительного расследования) и в рамках ДОУ (а не при расследовании уголовного дела). При этом исследуемые операции не тождественны и оперативно-розыскным операциям, поскольку последние рассматриваются в большинстве случаев как организационная форма проведения сложных ОРМ «оперативный эксперимент», «контролируемая поставка» и «оперативное внедрение».

УДК 343.3/7

В.И. Пикта

ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ В КОНТЕКСТЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Функционирование современного общества неразрывно связано с использованием широкого спектра различного программного обеспечения, начиная от операционных систем, веб-браузеров и заканчивая текстовыми процессорами и почтовыми клиентами. При таком широком использовании программных решений возникает постоянная потребность в обеспечении безопасности информационных систем.

Статистические данные, опубликованные на официальном сайте АО «Лаборатория Касперского» (www.kaspersky.ru) в текущем году, свидетельствуют о существенном росте количества уникальных киберинцидентов в сфере информационной безопасности. Так, за 2020 г. по отношению к 2019 г. их число выросло на 51 %, при этом большинство носило целенаправленный характер. Наиболее привлекательными объектами для компрометации выступали информационные системы государственных органов, медицинских учреждений и промышленных предприятий.

Перевод значительного числа работников на удаленную работу и вывод внутренних сервисов компаний за сетевой периметр спровоцировали рост спроса среди пользователей теневого сегмента сети Интернет на предоставление доступа к информационным системам компаний посредством несанкционированного доступа к их веб-ресурсам. Немногим организациям, которые и ранее практиковали удаленную работу, удалось преодолеть сложности в обеспечении требуемого уровня информационной безопасности, остальные же из-за нехватки времени на продумывание и реализацию мер защиты были вынуждены работать в условиях повышенной опасности для своих внутренних сервисов.

Одним из основных инструментов, используемых злоумышленниками в ходе осуществления несанкционированного доступа к информационным системам, выступают шифровальщики, вредоносное программное обеспечение (ВПО) для удаленного управления, автозагрузочное ВПО, шпионское и рекламное программное обеспечение, программы-майнеры, банковские трояны и др. Наиболее распространенными из них (более 75 % от общего числа) являются шифровальщики, функционал которых позволяет удаленно шифровать пользовательские данные жертв киберпреступлений и тем самым модифицировать и блокировать доступ к компьютерной информации. Обязательным условием расшифровки данных является перевод денежных средств, как правило, в виде криптовалюты.

Преобладающим мотивом осуществления вредоносных атак с использованием ВПО является корысть, получение финансовой выгоды.

Объектами посягательства с использованием ВПО выступают персональные компьютеры, серверное и сетевое оборудование, интернет-ресурсы, мобильные устройства, IT-устройства. Конечной целью атак с использованием ВПО на информационные системы в большинстве случаев выступает информация о персональных данных пользователей, авторизационные данные, информация, составляющая коммерческую тайну, клиентские базы данных организаций, электронная корреспонденция, а также данные платежных средств пользователей.

При этом разработчики ВПО постоянно изыскивают новые возможности для обхода существующих систем защиты программных продуктов. Для достижения поставленных целей они, как правило, используют редкие языки программирования, сигнатуры которых ввиду их незначительной распространенности пока еще не добавлены в базы существующих антивирусных программных решений, в связи с чем последние не могут обнаружить ВПО на устройстве. Некоторые злоумышленники дополняют свои инструменты функциями, позволяющими в режиме реального времени очищать следы вредоносной активности программы на устройстве жертвы.

Структурное строение способов совершения преступлений с использованием ВПО характеризуется тем, что они, как правило, относятся к разновидности полноструктурных, включающих в себя подготовку, совершение и маскировку (сокрытие) преступлений. Так, на этапе подготовки ВПО используется для собирания установочной информации о жертве, получения общих реквизитов платежных средств (номер банковской платежной карточки с маской, срок действия и имя владельца). На стадии совершения ВПО используется для получения авторизационных данных непосредственно в платежных системах либо перехвата сеансовых ключей, необходимых для удостоверения финансовых операций. Стадия маскировки (сокрытия) данных криминальных деяний характеризуется использованием средств анонимизации: VPN-сервисов, TOP-браузеров, удаленных анонимных серверов, бот-сетей и др.

Основным способом распространения ВПО является компрометация легитимных веб-ресурсов. Например, злоумышленники внедряют шпионское программное обеспечение в инструментальные средства, предназначенные для веб-разработки и устанавливаемые всеми разработчиками данной сферы. В дальнейшем это позволяет злоумышленникам удаленно собирать информацию об устройствах разработчиков и более предметно осуществлять целевые атаки. Среди способов встречаются случаи распространения ВПО посредством размещения его на крупных онлайн-площадках, предназначенных для инсталляции программного обеспечения на мобильные и десктопные устройства, например AppStore и PlayMarket.

Таким образом, ландшафт угроз в сфере использования ВПО достаточно широк. Функционал ВПО постоянно совершенствуется, а реагировать на существующие угрозы становится все сложнее. Специфика оборота ВПО, многообразие способов его создания, распространения и использования, недостаточная разработанность теоретической модели такого вида противоправных деяний создают существенные предпосылки для роста киберпреступлений в целом, в связи с чем имеется необходимость в разработке научно обоснованных практических рекомендаций по противодействию оборота ВПО.

УДК 343.985.8

С.В. Пилюшин

ОСОБЕННОСТИ АНАЛИЗА ИНФОРМАЦИИ, ПОЛУЧАЕМОЙ ОПЕРАТИВНЫМИ ПОДРАЗДЕЛЕНИЯМИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Деятельность оперативных подразделений органов внутренних дел по сбору, анализу, систематизации, хранению и последующему использованию оперативно-розыскной информации о лицах и фактах, представляющих оперативный интерес, рассматривается как информационное обеспечение, заключающееся в обеспечении оперативных подразделений оперативно-розыскной информацией и прикладным инструментарием для ее аналитической обработки.

Выступая в качестве одного из элементов информационного обеспечения, в теории оперативно-розыскной деятельности (ОРД) под оперативно-розыскной информацией понимают разновидность социальной информации, специфичной по цели получения, методам получения и режиму использования, обеспечивающего конспирацию и зашифровку ее источников. В ней могут находить свое отражение отношения между людьми, формирование преступного поведения, возникновение ситуаций, облегчающих или затрудняющих получение этой информации. Многообразие получаемой оперативно-розыскной информации коррелирует с многообразием обстоятельств, детерминирующих преступность и индивидуальное преступное поведение.

Оперативно-розыскная информация может быть получена из различных источников: обращения граждан; сообщения в средствах массовой информации; результаты проверок, проводимых контрольно-ревизионными органами, и др. Однако в большинстве случаев получению оперативно-розыскной информации предшествуют целенаправленные действия оперативных сотрудников по обнаружению, сбору, обработке, анализу и оценке фактических данных, содержащих сведения о замышляемых, подготавливаемых и совершенных преступлениях; лицах, представляющих оперативный интерес для органов внутренних дел; обстоятельствах, имеющих непосредственное или потенциальное значение для планирования или осуществления оперативно-розыскных мероприятий (ОРМ), проведения оперативно-аналитической работы.

По своему целевому назначению, исходя из полноты содержания, оперативно-розыскная информация может быть реализована при решении конкретной оперативно-розыскной задачи. Однако в большинстве случаев в ходе осуществления ОРД, как правило, требуется проведение ряда дополнительных операций по многим направлениям (переработка полученной информации, ее систематизация, хранение, поиск, выдача и т. д.), имеющим значение не только в настоящее время, но и в будущем. С этой целью и создаются различные по содержанию учеты.