«в будущее» оперативно-розыскное обеспечение процесса расследования, осуществляемое по инициативе оперативного сотрудника.

Определяя гносеологическую природу оперативно-розыскных мероприятий, необходимо отметить, что в отличие от следственных действий преступные действия, направленные на подготовку либо совершение экономического преступления, фиксируются непосредственно в момент их реализации и отражаются в делах оперативного учета. Причем содержание сведений о преступлении, полученных в результате осуществления ОРД, как правило, идентично сведениям, полученным в результате следственного действия. Однако их нельзя отождествлять, так как они отличаются задачами, стоящими перед ними, процедурой их организации и проведения, полномочиями участников и т. д. В связи с чем встает вопрос: что мешает объединить усилия следователей и оперативных сотрудников в решении задач борьбы с преступностью, исключив дублирование процессуальных функций?

В настоящее время в уголовно-процессуальном законодательстве Республики Беларусь отсутствуют прямые указания на использование материалов ОРД в качестве оснований для возбуждения уголовного дела, но наличествует термин «достаточные данные». Причем законодатель не раскрывает указанное понятие.

В связи с чем в практической деятельности часто возникают ситуации, когда оценка достаточности, сделанная оперативным сотрудником, не совпадает с оценкой достаточности, данной следователем. Вследствие чего, если последний посчитает, что собранных материалов недостаточно, такой материал возвращается оперативному сотруднику для проведения дополнительной проверки с указанием обязательных для выполнения мероприятий. При этом особо следует отметить ситуации, когда материал проверки стал результатом предварительно проведенного комплекса оперативно-розыскных мероприятий и промедление с принятием решения о возбуждении уголовного дела неизбежно приведет к потере интеллектуальных и материальных следов.

Отсутствие четкой правовой регламентации привело к тому, что на стадии возбуждения уголовного дела сотрудники подразделений по борьбе с экономическими преступлениями органов внутренних дел вынуждены устанавливать все элементы состава преступления, в том числе субъекта и субъективную сторону, хотя решение таких задач не является прерогативой стадии возбуждения уголовного дела.

Кроме оценки достаточности информации для принятия решения о возбуждении уголовного дела важной является оценка источников информации, которая позволяет по-новому взглянуть на работу с полученными сведениями. В криминалистическом аспекте традиционно

источники информации делятся на установленные в процессуальных и непроцессуальных формах. Они могут дополнять друг друга или вытекать один из другого. Такое общепризнанное деление не раскрывает свойств и ценности источников оперативно-розыскной информации и не показывает перспектив его возможного использования.

Применительно к решению проблем стадии возбуждения уголовного дела источники оперативно-розыскной информации представляют ценность, если содержат информацию о рассматриваемом событии и могут использоваться в уголовном процессе.

В результате сложившейся практики работы с материалами, используемыми в доказывании по уголовному делу, когда нередко происходит дублирование одних и тех же по содержанию познавательных действий, страдают все заинтересованные стороны в указанном процессе – и подразделения по борьбе с экономическими преступлениями органов внутренних дел, осуществляющие ОРД, и они же, проводящие доследственную проверку, следователи, расследующие уголовные дела, свидетели, граждане, права которых были нарушены в результате совершения преступления. Следует указать и на значительные финансовые затраты государства в связи с многократными вызовами и процедурами проведения оперативно-розыскных мероприятий и следственных действий.

В настоящее время сведения и следы преступления, установленные в ходе ОРД, не являются доказательствами. Для того чтобы стать таковыми, они должны быть восприняты субъектом доказывания с соблюдением надлежащей процедуры, отображены в его сознании, преобразованы им и уже в новом виде закреплены в материалах уголовного дела.

По нашему мнению, для повышения эффективности взаимодействия следователя и оперативного сотрудника необходимо по-новому взглянуть на место, роль, а также порядок использования материалов ОРД в уголовном процессе, что позволит уйти от двойного удостоверения фактических данных, имеющих одну и ту же познавательную сущность.

УДК 004.056

С.Ю. Воробьёв, Д.А. Жук, В.А. Русак, В.А. Шкред

МЕРЫ ПРОТИВОДЕЙСТВИЯ ЦИФРОВЫМ УГРОЗАМ В БАНКОВСКОЙ ОТРАСЛИ

Успешное развитие направлений банковской деятельности в настоящее время невозможно без серьезного наращивания информационной инфраструктуры банков и цифровизации процессов.

Кражи данных банковских платежных карт (банковских счетов) или данных доступа к системе интернет-банкинга с целью завладения средствами клиентов банка, кражи персональных данных и коммерческой информации из частных компьютеров или серверов, умышленное повреждение информационных систем или средств коммуникаций с целью создания убытков компаниям – далеко не полный перечень угроз, связанных с развитием информационных технологий.

Наиболее привлекательна для преступников банковская сфера, ведь она осуществляет ежедневно огромное количество транзакций и оборот значительных сумм денежных средств. Возможность получения баснословных доходов в случае успеха и достаточно невысокий уровень риска быть обнаруженными благоприятствуют росту киберпреступлений. Злоумышленники приспосабливаются к изменениям обстановки в сфере информационной безопасности, тщательно отслеживают появление новых уязвимостей в программном обеспечении и появление брешей в информационных системах банков и финансовых организаций.

Так, банковская система Республики Беларусь находится в поле зрения злоумышленников и международных преступных группировок. В последние несколько лет постоянно выявлялись факты мошенничества с использованием электронных платежных средств, имели место хакерские атаки на банки Республики Беларусь, в результате которых злоумышленниками похищались значительные денежные средства. Сотрудниками правоохранительных органов на территории Республики Беларусь задерживались участники международных преступных группировок Cobalt, Andromeda и др.

Национальный банк Республики Беларусь поддерживает и стимулирует обновление имеющихся и применение новых технических средств, систем и технологий обработки информации банками страны. Серьезное внимание уделяется регулированию вопросов обеспечения кибербезопасности банковской отрасли. В Национальном банке создан центр мониторинга и реагирования на компьютерные угрозы в банковской сфере Республики Беларусь (FinCERTby), основной задачей которого является организация, координация и осуществление оперативного взаимодействия Национального банка с банками и иными организациями по вопросам противодействия кибератакам.

На основе анализа мировой практики можно выделить следующие наиболее характерные для банковской сферы виды киберугроз на мировом уровне:

воздействие через аппаратные уязвимости – слабости, присутствующие в микропроцессорах разных производителей, открывающие новые возможности для злоумышленников, неустранимые при помощи программных обновлений;

компьютерный шпионаж – долговременное присутствие в сетях объектов критической информационной инфраструктуры с целью саботажа и шпионажа за деятельностью финансовых организаций;

целенаправленные кибератаки – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи банка, используемые для организации взаимодействия таких объектов, в целях проникновения в сеть конкретных банков и изолированные финансовые системы для вывода денежных средств;

клиентоориентированные кибератаки – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи банка, используемые для организации взаимодействия таких объектов, в целях хищения денежных средств конкретных клиентов или групп клиентов банка.

Выбор киберпреступниками целей обусловлен их технической подготовкой, имеющимся в наличии инструментарием и знаниями о внутренних процессах банка. При этом, как правило, основным фактором таргетированной атаки на финансовую организацию является слабая защита информационных систем.

Для успешного отражения банками кибератак необходимо выполнение ими следующих мер:

создание информационной инфраструктуры, позволяющей должным образом обеспечить информационную безопасность;

независимость подразделения киберзащиты от профильных ИТ-подразделений;

использование соответствующих аппаратных, программных и программно-аппаратных комплексов средств защиты информации;

мониторинг событий безопасности;

постоянное повышение квалификации работников, отвечающих за информационную безопасность (организация работы по получению ими сертификатов международного образца в области обеспечения кибербезопасности, например Certified Ethical Hacker, Certified Information Systems Security Professional);

обучение работников банков основам информационной безопасности;

включение пункта, связанного с соблюдением требований локальных правовых актов банка в сфере информационной безопасности, в трудовой договор;

поддержание здорового климата в коллективе (довольный работник с меньшей долей вероятности осознанно навредит организации, в которой работает);

информирование и обучение клиентов банков финансовой и цифровой грамотности;

разработка пакета нормативной документации, регламентирующей сферу информационной безопасности в банке (политика безопасности, регламент управления инцидентами и т. д.);

установление процедур обеспечения конфиденциальности информации;

создание команды по расследованию инцидентов информационной безопасности из числа наиболее подготовленных работников;

стандартизация бизнес-процессов;

скрупулезный подбор персонала в банковские организации с учетом их профессиональных, нравственных и моральных качеств;

регламентация порядка управления проектами по разработке, приобретению, внедрению новых и (или) обновлению имеющихся объектов информационной инфраструктуры;

создание дублирующих и резервных объектов информационной инфраструктуры;

внедрение в эксплуатацию автономных систем электропитания;

страхование рисков;

взаимодействие и обмен информацией о кибератаках между банками, правоохранительными органами и организациями, осуществляющими помощь в борьбе с угрозами цифрового пространства;

разработка и ввод в действие планов обеспечения непрерывности деятельности (в международной практике приемлемым считается восстановление безопасного функционирования банка в течение 2 ч с момента его прекращения).

Создание современной и надежной системы информационной безопасности и соблюдение требований норм последней всеми участниками информационного обмена являются залогом доверия не только к конкретной кредитно-финансовой организации, но и ко всей банковской системе государства.

УДК 343

В.В. Габбасова

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПНОСТИ В СФЕРЕ ГОСУДАРСТВЕННЫХ ЗАКУПОК ДЛЯ ОБЕСПЕЧЕНИЯ НУЖД ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Сфера государственных закупок чрезвычайно подвержена криминальным посягательствам. Субъектами противоправной деятельности могут выступать в том числе сотрудники ОВД, которые обязаны защи-

щать интересы государства. Такие преступления негативно влияют на доверие граждан как к правоохранительной системе, так и к государственной власти в целом, а также способствуют профессиональной деформации сотрудников ОВД, участвующих в организации и контроле закупочной деятельности для нужд обеспечения ОВД.

ОВД РФ – федеральный орган исполнительной власти, который нуждается в определенных товарах и услугах в связи со служебными потребностями.

Согласно приказу МВД России от 5 марта 2014 г. № 135 «Об организации материально-технического обеспечения в системе Министерства внутренних дел Российской Федерации» под материально-техническими средствами понимаются оружие, патроны к нему, боеприпасы, инженерные и специальные средства, средства радиационной, химической и биологической защиты, инженерно-технические средства укрепленности, технические средства охраны (в том числе системы охранной сигнализации, контроля и управления доступом, досмотра, охранного освещения, средства и системы оповещения), средства связи, инженерно-технические средства объектов связи, вычислительная, электронная организационная техника, аппаратно-программные комплексы, системы видеонаблюдения различного назначения, криптографические, шифровальные средства и технические средства защиты информации, криминалистическая техника, оперативная и специальная техника, авто- и бронетехника, водный транспорт, судовое оборудование, комплектующие, запасные части и расходные материалы, продовольствие, вещевое имущество, оборудование и технические средства продовольственной и вещевой служб, горюче-смазочные материалы, котельно-печное топливо, пожарно-техническая продукция, обозное имущество, альпинистское снаряжение, производственно-техническое и хозяйственное имущество, оборудование, мебель, расходные эксплуатационные и ремонтно-строительные материалы и другое имущество квартирно-эксплуатационной службы, медицинские изделия и лекарственные препараты, ветеринарное, спортивное оборудование, пищевой спирт, предметы для содержания служебных животных, ткани и другие положенные по нормам материальные средства. Под материально-техническим обеспечением понимается комплекс мероприятий, организуемых и осуществляемых в целях своевременного и полного удовлетворения потребностей ОВД РФ, организаций и подразделений, созданных для выполнения задач и осуществления полномочий, возложенных на МВД России.

Правовое регулирование государственной закупочной деятельности для обеспечения нужд ОВД основывается на Конституции Российской