другие источники доказательств, что вполне согласуется с требованиями Уголовно-процессуального кодекса Республики Беларусь (УПК).

О взаимодействии правоохранительных органов, осуществляющих борьбу с преступностью, в контексте выявления и преодоления противодействия раскрытию и расследованию преступлений необходимо вести речь с позиции не только использования в указанных целях средств, приемов и методов ОРД, но и использования специальных знаний. Особое значение имеет содействие специалистов в выявлении и преодолении противодействия раскрытию и расследованию преступлений, оказываемого на источники и носители вербальной доказательственной информации, связанного с попытками ее искажения, что невозможно осуществить посредством применения технических средств. В первую очередь это касается специальных знаний для диагностирования признаков противодействия, проявляющихся в речи, поведении и состоянии участников следственных действий. Такие знания позволяют оценить поведенческие реакции и показания, даваемые лицом, и на основании этого делать выводы о степени и формах оказанного воздействия.

Как отмечают В.Н. Карагодин и Ф.В. Балеевских, специальные знания в области психологии целесообразно использовать для установления свойств личности и особенностей мотивации противоправных действий субъекта противодействия, составления психологических портретов преступников, установления наличия и характеристики взаимоотношений между соучастниками преступлений и др. Несмотря на то что полученную таким путем информацию можно рассматривать лишь как ориентирующую в процессе расследования, тем не менее ее наличие помогает следователю определить направление работы по преодолению противодействия: разработать в этих целях общие и частные версии, сформировать систему мер и тактических особенностей их реализации.

Формами реализации специальных знаний в целях выявления и преодоления противодействия раскрытию и расследованию преступлений являются: дача заключений по результатам экспертиз, привлечение специалистов к проведению следственных и иных процессуальных действий, проведение исследований, оказание содействия в проведении следственных и иных процессуальных действий, допросы экспертов и специалистов в ходе предварительного следствия и в суде.

В Республике Беларусь прямого указания в законодательстве на то, что показания и заключения специалиста могут являться доказательствами по уголовному делу, нет, однако содержание ч. 2 ст. 88 УПК позволяет к ним отнести данные, полученные от указанных лиц. Активное использование в практической деятельности такой формы реализации

специальных знаний позволяет минимизировать оспаривание защитниками выводов, сделанных экспертами и специалистами.

Помощь специалиста как источника ориентирующей информации в целях преодоления противодействия раскрытию и расследованию преступлений наиболее важна оперативным сотрудникам. Выполняемые ими функции, по сути, однотипны с действиями, которые специалисты осуществляют при производстве процессуальных действий, однако в ходе осуществления ОРД возможности применения специальных знаний в нетрадиционных областях, к числу которых относятся гипноз, экстрасенсорика и др., значительно шире.

Подводя итог, необходимо подчеркнуть, что взаимодействие правоохранительных органов в системе выявления и преодоления противодействия раскрытию и расследованию преступлений выступает одним из ключевых элементов. Основу такого взаимодействия составляют контакты и отношения, выстраиваемые субъектами в ходе решения совместных задач в сфере борьбы с преступностью.

УДК 338.2

Е.Н. Мисун, А.А. Ластовский

ОСНОВНЫЕ УГРОЗЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ В ЦИФРОВОМ ПРОСТРАНСТВЕ

Современный мир характеризуется динамичными глобальными процессами. Прогресс информационных технологий обусловил расширение сфер применения мобильных устройств, дистанционных платежей, интернет-банкинга, что, в свою очередь, создало предпосылки для их использования в преступных целях и привело к значительному росту преступлений в IT-сфере, а также к появлению новых форм противоправной деятельности, связанных с использованием компьютерных сетей для совершения и сокрытия преступлений. Преступные группы активно используют в своей деятельности достижения науки и техники, применяют всевозможные компьютерные устройства и новые информационно-обрабатывающие технологии.

Преступления против экономической безопасности приобрели сегодня транснациональный, организованный и групповой характер. С использованием телекоммуникационных сетей и компьютера противоправное деяние может быть совершено не выходя из квартиры или офиса, на территории другой страны и даже нескольких государств одновременно.

Повышенный интерес злоумышленников к сети Интернет связан с тем, что она не находится в ведении конкретного физического лица, частной компании, государственной или общественной организации и даже отдельной страны. Существующие на сегодня формы контроля не обеспечивают полной защиты информации, что позволяет осуществлять несанкционированный доступ к ней. Вышеизложенное позволяет говорить о расширении сфер применения информационных технологий в криминальной деятельности в цифровом пространстве.

Республика Беларусь, как и все мировое сообщество, ориентирована на развитие безналичных расчетов, сопровождающихся увеличением числа устройств для осуществления финансовых транзакций, а также ростом числа пользователей всевозможных электронных дистанционных платежных систем. Не последнюю роль здесь играет и распространение коронавирусной инфекции COVID-19, спровоцировавшей переход в интернет-пространство многих сфер общественных отношений, включая удаленный режим работы, товарный и денежный обороты.

На протяжении последних лет в Республике Беларусь, как и во всем мире, наблюдалась устойчивая тенденция роста количества регистрируемых киберпреступлений. По данным официального интернет-портала Минского городского исполнительного комитета, в 2015 г. в республике было зарегистрировано около 2,5 тыс. киберпреступлений, а в 2020 г. – в 10 раз больше (свыше 25,5 тыс.). Негативная тенденция роста киберзлодеяний сохранилась и в первом полугодии 2023 г. – их зарегистрировано на 17 % больше, чем за аналогичный период прошлого года.

Как и ранее, основную часть из числа регистрируемых киберпреступлений составляют хищения имущества путем модификации компьютерной информации (около 83 %). В преступной мотивации по-прежнему превалируют экономические интересы, а жажда наживы остается основным мотивообразующим фактором формирования преступного замысла. Центральным звеном в сфере интересов киберпреступников остаются предприятия всех форм собственности, а также граждане Республики Беларусь, имеющие в наличии банковские платежные карточки.

Это довольно логично, так как Республика Беларусь активно движется в сторону развития системы электронных услуг и цифровых платежей. Так, по сравнению с 2011 г. в разы выросло количество организаций торговли, оснащенных платежными терминалами (с 18 тыс. до 148 тыс.). Сегодня почти 8 млн белорусов в той или иной степени пользуются Интернетом как посредником в оказании финансовых услуг, а согласно официальному сайту Национального банка Республики Беларусь белорусские банки выпустили в обращение почти 19 млн банковских платежных карточек (в 2011 г. – 9 млн).

В целях противодействия киберпреступлениям в сфере экономики необходимо постоянно повышать уровень взаимодействия между правоохранительными органами и банковскими учреждениями, так как часто от скорости и оперативности получения информации о движении денежных средств по банковским счетам зависит возможность установления личности злоумышленника и отмены транзакции, а также возврата похищенных денежных средств.

Следует отметить, что конкретные меры безопасности проведения операций при использовании реквизитов банковских платежных карточек в сети Интернет определяются банками самостоятельно с учетом требований законодательства, правил платежных систем и принятой в банке политике информационной безопасности.

Можно выделить следующие наиболее эффективные меры по противодействию экономическим киберпреступлениям, предпринимаемые сегодня банковскими учреждениями:

обязательное подтверждение операций, совершаемых держателями банковских платежных карточек с применением их реквизитов в сети Интернет (технология 3D-Secure);

установление банком-эмитентом ограничений по проведению расходных операций (максимальная сумма и количество операций в определенный период времени);

предоставление держателю банковской платежной карточки возможности самостоятельно устанавливать индивидуальные ограничения (лимиты, запреты) на проведение финансовых операций;

использование систем автоматического выявления подозрительных операций, совершенных при использовании банковских платежных карточек (системы фрод-мониторинга).

Как свидетельствует практика, установление индивидуальных ограничений, лимитов и запретов самим держателем банковской платежной карточки является сегодня наиболее эффективным способом обеспечения сохранности размещаемых на счетах клиентов денежных средств. Как правило, такие ограничения можно устанавливать дистанционно. Конкретные виды ограничений и лимитов, виды операций, а также география совершения платежей в индивидуальном порядке предлагаются банками, выпустившими карточку в обращение.

Говоря о персональной безопасности при проведении финансовых операций в сети Интернет, следует подчеркнуть необходимость соблюдения пользователями базовых правил «цифровой гигиены». К ним относятся следующие:

персональную информацию и платежные реквизиты следует тщательно оберегать от возможного несанкционированного доступа третьих лиц;

необходимо соблюдать правила безопасности при совершении финансовых операций в сети Интернет (не сохранять автоматически пароли, пользоваться только проверенными программами и браузерами, не открывать подозрительные объекты, не переходить по ссылкам, полученным от неизвестных лиц);

следует содержать в «цифровой чистоте» персональные устройства ввода и хранения конфиденциальной информации (регулярно обновлять антивирусное программное обеспечение, своевременно обновлять операционную систему, следить за предоставлением доступа к персональной информации, периодически менять пароли);

ни в коем случае не передавать третьим лицам персональную информацию и реквизиты банковских платежных карточек.

Подводя итог, следует отметить, что вопросы цифровой трансформации современной преступности являются сегодня наиболее злободневными для экономической безопасности государства в целом. Однако универсальных подходов, позволяющих эффективно противодействовать высокотехнологичным преступлениям, не выработано на данный момент ни одной страной в мире.

Очевидно, что тенденции дальнейшей цифровизации криминальной деятельности будут в обозримом будущем оказывать определяющее воздействие на деятельность правоохранительных органов. От того, насколько эффективно государство сможет противостоять этому вызову, зависит состояние не только правопорядка, защищенности прав и интересов граждан, но и экономической безопасности Республики Беларусь в целом.

УДК 349.233

С.А. Орлова

ОСОБЕННОСТИ ВЗЫСКАНИЯ С РАБОТНИКОВ МАТЕРИАЛЬНОГО УЩЕРБА, ПРИЧИНЕННОГО НАНИМАТЕЛЮ ПРИ ИСПОЛНЕНИИ ТРУДОВЫХ ОБЯЗАННОСТЕЙ

Постановлением Пленума Верховного Суда Республики Беларусь от 26 марта 2002 г. № 2 «О применении судами законодательства о материальной ответственности работников за ущерб, причиненный нанимателю при исполнении трудовых обязанностей» определено, что материальная ответственность работников является самостоятельным видом юридической ответственности, предусматривающей обязанность работника возместить в установленных законодательством случаях, порядке

и размерах ущерб, причиненный нанимателю при исполнении трудовых обязанностей, и наступающей независимо от привлечения работника за противоправное поведение к дисциплинарной, административной или уголовной ответственности.

Материальная ответственность сотрудников органов внутренних дел регламентируется Положением о материальной ответственности лиц рядового и начальствующего состава органов внутренних дел Республики Беларусь, утвержденным постановлением Совета Министров Республики Беларусь от 27 августа 2012 г. № 789.

В 2021 г. судами было рассмотрено более 207 тыс. гражданских дел, из них более 7,5 тыс. касались трудовых споров, при этом более трети трудовых споров составляли дела о материальной ответственности работников. Следует отметить, что такое примерное количество трудовых споров, касающихся вопросов возмещения материального ущерба за вред, причиненный нанимателю, сохраняется на протяжении последних пяти лет.

Более 80 % всех споров рассмотрены с вынесением решения, причем в основном исковые требования удовлетворяются. Как правило, наниматели обоснованно предъявляют к работникам требования о возмещении причиненного по их вине ущерба.

Необходимо отметить, что с каждым годом фиксируется незначительная тенденция к увеличению количества рассмотренных судами дел о возмещении ущерба, при этом по-прежнему более 90 % исковых требований удовлетворяются. Число апелляционных жалоб за последние годы сокращается. Количество удовлетворенных исковых требований достаточно велико, в то же время качество рассмотрения подобных дел улучшается из года в год.

Суммы, которые наниматели предъявляют к взысканию, являются значительными, и сохраняется тенденция на их увеличение. Вместе с тем согласно статистике суды реально взыскивают около 50 % от всей заявленной суммы ежегодно. Так, в 2021 г. к взысканию было предъявлено 13 млн 802 тыс. р. Удовлетворено – на 7 млн 232 тыс. р. Такая ситуация складывается за счет того, что у суда есть возможность уменьшить сумму ущерба, подлежащую к взысканию с работника, с учетом конкретных обстоятельств дела, степени вины ответчика, его материального положения.

П. 7 ст. 42 Трудового кодекса Республики Беларусь (ТК) предусматривает, что трудовой договор, заключенный на неопределенный срок, а также срочный трудовой договор до истечения срока его действия могут быть расторгнуты нанимателем в случаях однократного грубого нарушения работником трудовых обязанностей, в том числе за наруше-