юстиции, входящими в него ФБР и Национальной объединенной рабочей группой по киберрасследованиям.

Министерство внутренней безопасности противодействует киберугрозам, разрешает киберинциденты с помощью Национального центра интеграции кибербезопасности и связи.

Управление директора национальной разведки, используя возможности Центра интеграции информации о киберугрозах, является главным федеральным органом их разведывательного обеспечения, сопровождения и нейтрализации.

Европейская модель направлена на реализацию утвержденной странами Европейского союза стратегии обеспечения кибербезопасности, осуществляемой на союзном и государственном уровнях. Данная модель отличается более продуманным и организованным комплексом мероприятий, проводимых в рассматриваемом контексте (разработка концепции киберустойчивости организаций и объектов к киберинцидентам различного содержания, длительности и интенсивности, законодательное, организационное, методическое, материально-техническое, кадровое и финансовое сопровождение).

Активно осуществляется формирование в сознании граждан культуры кибербезопасности, алгоритмизации реагирования пользователей Сети на возможные ухищрения, используемые киберпреступниками (фишинговые письма, программы-шифровальщики, программные вирусы и др.). В этих целях проводится системная разъяснительная работа, так называемые ежегодные месячники кибербезопасности, повышающие уровень знаний и навыков должностных лиц и граждан в сфере кибербезопасности.

Обеспечением кибербезопасности в соответствии с принятым в 2019 г. специальным законом занимаются не только специализированные государственные структуры в сфере IT-технологий (Агентство Европейского союза по сетевой и информационной безопасности, осуществляющее информационно-аналитические и практические мероприятия по предупреждению, выявлению и разрешению киберинцидентов), но и общественные организации, онлайн-сообщества, бизнес-структуры, исследовательские и образовательные учреждения.

Зарекомендовал себя с положительной стороны созданный восемь лет назад Европейский центр борьбы с киберпреступностью, внесший значительный вклад в борьбу с этим криминальным явлением, его резонансными проявлениями на территории государств Евросоюза.

Следует обратить особое внимание на вопросы материально-технического обеспечения реализации стратегии кибербезопасности государств Европейского союза в постпандемийный период, а также их финансирования, исчисляемого почти 2 млрд евро.

В ходе исследования нами также определены другие модели обеспечения кибербезопасности: китайская (КНР), стран Юго-Восточной Азии (Южная Корея, Сингапур, Индонезия и Малайзия), а также государств, ориентированных на национальный, государственный интернет (Иран, КНДР).

Таким образом, рассмотренные основные модели свидетельствуют об озабоченности и приоритетности деятельности органов законодательной и исполнительной власти различных государств, институтов гражданского общества и бизнеса по созданию, внедрению и развитию современных форм и методов противодействия киберпреступности, обеспечения кибербезопасности.

УДК 343.985

А.А. Ковальчук

О ВЗАИМОДЕЙСТВИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ И ПРЕДСТАВИТЕЛЕЙ БАНКОВСКОГО СЕКТОРА В КОНТЕКСТЕ БОРЬБЫ С ХИЩЕНИЯМИ, СОВЕРШАЕМЫМИ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ ПЛАТЕЖНЫХ КАРТОЧЕК И ИХ РЕКВИЗИТОВ

Официальная статистика МВД Республики Беларусь показывает, что в 2020 г., как и в предыдущие годы, растет количество хищений, совершенных путем использования компьютерной техники (ст. 212 УК Республики Беларусь). Значительную часть среди них составляют хищения, совершенные с использованием реквизитов банковских платежных карточек (БПК). Для завладения реквизитами злоумышленники чаще всего используют методы социальной инженерии посредством телефонных и интернет-коммуникаций, а также так называемые фишинговые интернет-ресурсы.

Возможность совершения хищений в ряде случаев обусловлена неосмотрительностью со стороны держателей БПК. Невзирая на комплекс профилактических мероприятий, проводимых ГУПК КМ МВД Республики Беларусь в средствах массовой информации, в том числе в сети Интернет, держатели БПК продолжают допускать ошибки, приводящие в дальнейшем к совершению хищений.

Указанное требует от представителей банковского сектора принятия соответствующих мер реагирования, направленных на усиление защиты клиентов банков от противоправных посягательств. В этой связи ГУПК КМ МВД на основе всестороннего изучения существующих проблем подготовлен актуальный комплекс мер, включающий:

исключение размещения информации о CVV-коде на поверхности БПК, передачу ее держателю на бумажном носителе, упакованном в специальный защитный конверт, либо посредством СМС-сообщения (по аналогии с PIN-кодом);

запрет опции по умолчанию для интернет-платежей по эмитированным БПК с возможностью подключения данного функционала при выдаче карточки (по желанию держателя) либо его активации посредством системы дистанционного банковского обслуживания (СДБО) с подтверждением действий путем ввода защитного кода 3D-Secure;

одновременное подключение по умолчанию технологии 3D-Secure при активации держателем БПК функции совершения интернет-платежей (в том числе посредством СДБО), за исключением платежей, совершаемых в адрес государственных учреждений (оплата коммунальных услуг, штрафов и др.);

установка рациональных ограничений по сумме и количеству совершаемых в определенный период операций, связанных с P2P-переводами (со счета одной БПК на счет другой БПК с использованием их реквизитов в сети Интернет);

внедрение технологии графического пароля как дополнительного средства идентификации пользователя при проведении операций (в дополнение к используемой технологии 3D-Secure);

применение механизма биометрической аутентификации пользователей (статического – отпечаток пальца, геометрия руки, радужная оболочка глаза и др.; динамического – голос, динамика набора текста, динамика воспроизведения подписи и др.) при осуществлении доступа к СДБО и проведении платежей;

внедрение дополнительных правил системы фрод-мониторинга (от англ. fraud – мошенничество), позволяющих выявлять нетипичные (подозрительные) операции, приостанавливать их проведение на период, необходимый для реагирования клиента банка (от 20 минут до 1 часа), осуществлять информирование клиента о данных операциях, приостанавливать доступ к СДБО при обнаружении подозрительных операций.

Реализация представителями банковского сектора вышеуказанных мер, разработанных ГУПК КМ МВД, позволит решить ряд проблем, касающихся защищенности держателей БПК, что, в свою очередь, усложнит процесс совершения хищений путем использования компьютерной техники и, соответственно, обеспечит снижение их количества. В заключение стоит также отметить, что от степени и качества взаимодействия органов внутренних дел и представителей банковского сектора во многом зависит дальнейшее состояние борьбы с преступлениями рассматриваемого вида.

УДК 343.98

Ж.И. Ковган

ЭКОНОМИЧЕСКАЯ ЭКСПЕРТИЗА КАК ОДИН ИЗ ИНСТРУМЕНТОВ ПРОТИВОДЕЙСТВИЯ ЭКОНОМИЧЕСКОЙ ПРЕСТУПНОСТИ

Экономическая экспертиза – это один из видов судебных экспертиз. При ее проведении осуществляется системное исследование документов финансово-хозяйственной деятельности субъектов всех форм собственности и индивидуальных предпринимателей, по результатам которого делается соответствующий вывод. В свою очередь, заключение эксперта – это один из источников доказательств, оказывающих влияние на расследование экономических преступлений.

В заключении эксперт дает ответы на поставленные перед ним вопросы. Выводы могут быть категорическими, вероятными, о невозможности решения вопроса. Результат исследования и сроки его проведения зависят от характера вопросов, выносимых на разрешение эксперта, полноты и качества собранных материалов. Рассмотрим влияние указанных обстоятельств на ход экспертного исследования и формирования выводов.

Государственным комитетом судебных экспертиз Республики Беларусь разработаны рекомендации по назначению экономической экспертизы, которые направлены в правоохранительные и судебные органы. В них детально описаны объекты, основные задачи, круг решаемых вопросов, основные стадии экспертного исследования. Они также содержат основные требования к формулировке вопросов, выносимых на разрешение экономической экспертизы. Особое внимание в них уделено вопросам, которые не подлежат разрешению при проведении экономической экспертизы. Вместе с тем на практике имеют место ситуации, оказывающие влияние на формирование выводов эксперта в данной части.

В этой связи рассмотрим особенности формулирования вопросов, выносимых на разрешение экономической экспертизы, которые не относятся к ее задачам:

1. Выходящие за пределы специальных познаний эксперта-экономиста (сообщается о невозможности дачи заключения): вопросы правового характера, установление нарушений законодательства, установление законности совершения тех или иных операций, законности осуществления каких-либо действий, определение ущерба (материального ущерба, вреда), виновности, степени ответственности должностных и иных лиц, а также юридическая квалификация их действий (бездействия) и др. При этом с целью оказания всесторонней помощи экспер-