***A.I. Borodich**, PhD of law, associate professor, head of the department of border of the Institute of Homeland Security of the Republic of Belarus; **N.A. Vashkevich**, senior staff scientist of the Scientific Research Laboratory of general forensic and autotechnical research of the research department of forensic science research of the Scientific and Practical Centre of the State Committee of forensic examination of the Republic of Belarus; **P.I. Zhestkov**, head of the department of professional and vocational preparation of the second department of prime responsibility of the State Border Committee of the Republic of Belarus; **S.A. Shvedova**, head of the Department of planning, management, security and organizational support of 'Minsk' border control brigade of the State Border Committee of the Republic of Belarus*

USING BIOMETRIC TECHNOLOGIES FOR PROTECTION OF E-PASSPORT PERSONAL DATA AND AUTOMATED DOCUMENT VERIFICATION SYSTEM

Currently, in many countries the biometric technologies are used to protect e-passport personal data. However, until now, there is no accepted unique standard for the next generation of passports in the world; some countries introduce fingerprints into chips in the test mode, others – the iris image, the requirements for biometric characteristics in different countries are different, too. Therefore, the issues of using biometric technologies to protect e-passport personal data and the document check automated system at checkpoints on the State Border are still relevant. The article offers recommendations that may be useful for the introduction of e-passports in the Republic of Belarus.

Keywords: biometrics, e-passports, machine-readable passports, border control.

УДК 343.375

***Г.В. Глинский**, следователь по особо важным делам отдела по расследованию преступлений против интересов службы управления Следственного комитета Республики Беларусь по Гомельской области;*
***А.Э. Набатова**, кандидат юридических наук, доцент, начальник кафедры управления защитой от чрезвычайных ситуаций Гомельского инженерного института МЧС Республики Беларусь*

О КВАЛИФИКАЦИИ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ ПЛАТЕЖНЫХ КАРТОЧЕК

Рассматриваются проблемные вопросы квалификации хищений, совершаемых с использованием банковских платежных карточек. Авторами определены термины и определения, необходимые для правильной квалификации данных преступлений, проанализированы спорные аспекты с точки зрения уголовного права, возникающие при правовой оценке действий виновного. Рассмотрены ситуации, возникающие на практике, предложены алгоритмы их разрешения в правоприменительной деятельности.

Ключевые слова: преступление, хищение, банковская платежная карточка, процессинг, процессинговый центр, авторизация, кража, имущество, денежные средства.

По данным статистики в Республике Беларусь сохраняется общая тенденция к росту преступлений, совершаемых с использованием компьютерной техники (например, в 2007 г. было совершено 91 преступление, в 2009 г. – 325, 2012 г. – 310 и т. д.). Как показывает мировой опыт, данная проблема свойственна всем развитым государствам. Это объясняется объективными причинами. Во-первых, количество таких преступлений увеличивается в связи с бурным развитием информационных технологий. Во-вторых, стремительно растет перечень услуг, предоставляемых населению путем их использования.

Что касается платежных систем, действующих на территории Республики Беларусь, то необходимо отметить увеличение количества расчетов с использованием банковских платежных карточек (например, в 2012 г. было проведено 643 627 814 операций с использованием банковских платежных карточек). С их помощью происходит снятие денежных средств, расчет за приобретаемые товары и услуги на предприятиях торговли и сервиса, в сети Интернет. Описанные выше тенденции, с одной стороны, являются положительными и предоставляют гражданам новые возможности, с другой – неизбежно ведут к появлению новых видов, способов преступной деятельности.

Тенденцией сегодняшнего дня является совершение хищений с использованием компьютерной техники. Подавляющее большинство таких преступлений – это хищения с использованием банковских платежных карточек. В связи с вышеизложенным особую актуальность приобретают вопросы квалификации хищений, совершаемых с их помощью. Таким образом, объектом нашего исследования выступают закономерности деятельности уполномоченных субъектов по разрешению проблемных вопросов, связанных с квалификацией хищений, совершаемых с использованием банковских платежных карточек. В качестве предмета можно определить теоретические и прикладные аспекты квалификации данных преступлений (в частности, ст. 212 УК Республики Беларусь).

К вопросам квалификации хищений рассматриваемой категории на протяжении последнего десятилетия обращались ученые-юристы, среди которых можно отметить труды Д. Айкова [2], С. Воронцовой [1], В. Крылова [3], А. Лепехина [4], О. Петрухина [7], А. Расулева [8], Л. Устьева [9] и др. В контексте данной публикации рассматривать традиционные положения, связанные с юридической характеристикой объективных и субъективных признаков состава преступления, предусмотренного ст. 212 УК, представляется неце-

лесообразным, так как данной проблематике посвящено достаточно учебной и учебно-методической литературы.

Обратим внимание на некоторые дискуссионные вопросы. Во-первых, в ситуации, когда действия лица, совершающего хищение денежных средств с карт-счетов граждан с использованием поддельных банковских платежных карточек либо реквизитов к ним, проблем с квалификацией не возникает, и существует единое мнение, что указанные действия необходимо квалифицировать по ч. 2 ст. 212 УК в связи с наличием признака введения в компьютерную систему ложной информации. Во-вторых, предметом постоянных споров между органами предварительного расследования, прокуратуры и судов является квалификация действий лица, совершающего хищение денежных средств с применением подлинной банковской платежной карточки, выбывшей из законного пользования владельца карт-счета по различным причинам (потеря, хищение с целью последующего снятия денежных средств с карт-счета, оставление в банкомате после совершенных транзакций, добровольная передача во временное пользование лицу, которое впоследствии совершает хищение).

Таким образом, можно сформулировать два проблемных аспекта, при возникновении которых на практике возможны сложности в квалификации действий лиц, совершающих хищения с использованием банковских платежных карточек: 1) лицо совершает хищение с использованием подлинной банковской платежной карточки с введением ПИН-кода; 2) лицо совершает хищение с использованием банковской платежной карточки, осуществляя расчет за приобретенный товар на предприятиях торговли или сервиса без введения ПИН-кода.

Основные понятия и порядок совершения операций с банковскими платежными карточками описаны в Инструкции о порядке совершения операций с банковскими платежными карточками [6]. Обратимся к некоторым из них: авторизация – разрешение банка-эмитента и (или) владельца платежной системы на совершение операции при использовании карточки, сопровождающееся блокировкой денежных средств; банк-эмитент – банк, банк-нерезидент, осуществляющие эмиссию карточек и принявшие на себя обязательства по перечислению денежных средств со счетов клиентов в соответствии с условиями договоров об использовании карточек и (или) принявшие на себя обязательства по перечислению денежных средств в соответствии с условиями кредитных договоров, предусматривающих предоставление кредита при использовании кредитной карточки; банкомат – электронно-механический программно-технический комплекс, обеспечивающий выдачу и (или) прием наличных денежных средств, совершение других операций при использовании карточки, установленных банком и не противоречащих законодательству, регистрацию таких операций с последующим формированием карт-чека; ПИН-код – персональный идентификационный номер, используемый для идентификации держателя карточки; процессинг – деятельность по сбору и обработке информации, поступающей от организаций торговли (сервиса), банкоматов, платежно-справочных терминалов самообслуживания, пунктов выдачи наличных денежных средств либо из иных источников в зависимости от технологий, используемых участниками платежной системы, а также по передаче обработанной информации для проведения безналичных расчетов; процессинговый центр – юридическое лицо, в том числе банк, иностранная организация, не являющаяся юридическим лицом по иностранному праву, осуществляющие процессинг на основании договоров с иными участниками платежной системы, заключенных в соответствии с правилами платежной системы. Оборудование и программные средства, обеспечивающие процессинг, подпадают под понятие компьютерной системы.

В контексте заявленных положений необходимо определиться с ситуацией, когда лицо, совершающее хищение с использованием подлинной банковской платежной карточки, вводит ПИН-код через процессинговый центр, являющийся компьютерной системой. Будет ли в таком случае вводимая информация ложной для системы, ведь речь идет о неодушевленном объекте, который не имеет возможности определить, кто именно вводит информацию – владелец банковской платежной карточки или преступник.

Для того чтобы разобраться в подобных обстоятельствах, необходимо рассмотреть процесс получения денежных средств через банкомат. Он заключается в следующем. Банковская платежная карточка вставляется в банкомат, который является компьютерной системой, считывающей информацию с магнитной полосы карточки и передающей ее по компьютерной сети в компьютерную систему процессингового центра. Магнитная полоса карточки содержит данные, необходимые для идентификации личности владельца карточки при ее использовании в банкоматах и электронных терминалах торговых учреждений. Когда карточка вставлена в соответствующее считывающее устройство, индивидуальные данные владельца передаются по компьютерным сетям для получения разрешения на осуществление сделки – авторизации.

Для удостоверения факта использования карточки ее держателем компьютерная система процессингового центра запрашивает ПИН-код, который владелец карточки вводит с использованием имеющейся в банкомате клавиатуры. На данной стадии следует отличать характер вводимой информации в зависимости от того, кем она вводится – законным держателем карточки или преступником. Несмотря на то что по содержанию вводимая преступником информация является подлинной для компьютерной системы, в рамках действий лица, совершающего хищение с карт-счета, она носит заведомо ложный ха-

рактер, так как в систему вводится не принадлежащий преступнику идентификационный номер. Такой доступ в соответствии с п. 20 постановления пленума Верховного суда Республики Беларусь от 21 декабря 2001 г. № 15 «О применении судами уголовного законодательства по делам о хищениях имущества» является несанкционированным – доступ к компьютерной информации лица, не имеющего права на доступ к этой информации либо имеющего такое право, но осуществляющего его помимо установленного порядка [5].

Таким образом, хищения денежных средств из банкоматов при помощи банковских платежных карточек лицами, не являющимися их держателями, сопряжены с несанкционированным доступом к компьютерной информации о карт-счетах владельцев банковских платежных карточек и совершаются путем введения в компьютерную систему процессингового центра заведомо ложной информации об использовании карточек якобы их правомерными держателями. Подобные действия подлежат квалификации по ч. 2 ст. 212 УК.

Несмотря на приведенные аргументы, дискуссии по поводу ложности либо достоверности вводимой информации продолжаются. Многие ученые и практики считают, что если вводимая в процессинговый центр информация не является ложной, то действия виновного лица не должны быть квалифицированы по ст. 212 УК, однако при таких рассуждениях упускается тот факт, что диспозиция анализируемой статьи предусматривает два альтернативных действия, которые образуют самостоятельные составы хищения: 1) путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных; 2) путем введения в компьютерную систему ложной информации.

Отдельного внимания заслуживает юридическая оценка действий преступника, совершающего хищение денежных средств с использованием банковской платежной карточки, осуществляя расчет за приобретенный товар на предприятиях торговли или сервиса без введения ПИН-кода.

При осуществлении расчета с использованием банковской платежной карточки на предприятии торговли или сервиса происходит следующее: клиент после подсчета стоимости товаров или услуг предъявляет кассиру свою карточку; кассир осуществляет проверку принадлежности карты клиенту, например по образцу подписи на ней; кассир формирует авторизационный запрос в процессинговый центр; процессинговый центр, получив авторизационный запрос, проверяет наличие карты в стоплистах, по номеру карты определяет эмитента и пересылает ему этот запрос; эмитент, получив авторизационный запрос, осуществляет проверку на возможность клиента платить по карте, блокирует указанную в запросе сумму на карточном счете и дает подтверждение авторизации; процессинговый центр, получив ответ от эмитента, пересылает его на POS-терминал. В том случае, когда авторизация подтверждена, терминал распечатывает два экземпляра чека, которые подписываются клиентом – держателем карты, один экземпляр передается клиенту; в конце рабочего дня на POS-терминале формируется журнал операций за день (смену) в виде файла финансового подтверждения проведенных операций по оплате товаров с помощью карты, который отсылается в процессинговый центр и эквайреру. Процессинговый центр, получив файл финансового подтверждения, сортирует его по эмитентам и пересылает каждому эмитенту ту его часть, которая содержит номера карты этого эмитента. Одновременно процессинговый центр передает файл финансового подтверждения расчетному банку и банку-эквайреру; эмитент, получив от процессингового центра финансовое подтверждение, снимает блокировку со специальных карточных счетов по тем картам, номера которых присутствуют в файле, списывает указанные суммы с этих карточных счетов и перечисляет их в расчетный банк для зачисления на свой счет; расчетный банк на основании полученного файла финансового подтверждения списывает средства со счетов эмитентов и зачисляет их на счет эквайрера; эквайрер, получив выписку по своему счету в расчетном банке, зачисляет средства на счет предприятия, через POS-терминал которого была осуществлена операция оплаты по банковской платежной карточке.

Таким образом, при хищении денежных средств с карт-счета путем расчета с использованием банковской платежной карточки на предприятии торговли или сервиса происходит противоправное безвозмездное завладение чужим имуществом – хищение путем изменения информации, обрабатываемой в компьютерной системе, что приводит к уменьшению размера денежных средств, хранящихся на банковском карт-счете.

Что касается введения в компьютерную систему ложной информации, то необходимо отметить, что при помещении кассиром или продавцом предоставленной виновным лицом банковской платежной карточки в электронный торговый терминал в процессинговый центр по сетям передачи данных автоматически вводится информация о номере карточки, принадлежащей законному владельцу. Таким образом, процессинговый центр (компьютерная система) получает ложную информацию о пользователе карточки.

Кроме того, как уже указывалось выше, в соответствии с п. 20 постановления пленума Верховного суда № 15 бесспорным является тот факт, что виновное лицо, совершая незаконные операции с использованием банковской платежной карточки, осуществляет несанкционированный доступ к компьютерной информации о карт-счете законного держателя карточки [5].

Нередко при расследовании уголовных дел данной категории возникает сложность в квалификации действий преступника по совокупности совершенных им противоправных деяний. В данном случае необходимо руководствоваться ст. 42 УК и постановлением пленума Верховного суда № 15.

При расследовании уголовных дел данной категории часто возникает проблема в квалификации действий преступника, когда он осуществляет хищение банковской платежной карточки с проникновением в жилище. В таких ситуациях правоприменители нередко ссылаются на ч. 4 примечаний к гл. 24 УК, мотивируя тем, что, если хищение сопряжено с проникновением в жилище, размер ущерба не имеет значения для квалификации, следовательно имеет место хищение банковской платежной карточки, совершенное с проникновение в жилище, – ч. 2 ст. 205 УК. Тем не менее следует обратить внимание на то, что в указанной норме права законодатель предусмотрел наступление ответственности по ч. 2 ст. 205 УК независимо от размера причиненного вреда при хищении с проникновением в жилище только личного имущества физического лица.

Однако банковская платежная карточка является собственностью банковского учреждения (юридического лица), и ее стоимость не превышает 10-кратного размера базовой величины, которая устанавливается на день совершения преступления. Следовательно действия преступника не могут быть квалифицированы по ч. 2 ст. 205 УК. Как представляется, в описанной ситуации можно вести речь о квалификации действий по ст. 202 УК «Нарушение неприкосновенности жилища и иных законных владений граждан» и только при наличии заявления собственника в совокупности с хищением по ст. 212 УК в случае его совершения.

В случае когда лицо, завладевая чужой банковской платежной карточкой, намеревается похитить денежные средства, а при просмотре остатка на карт-счете убеждается, что баланс счета нулевой, и поэтому не доводит свои преступные действия до конца по независящим от него обстоятельствам, то его действия следует квалифицировать как покушение на хищение с использованием компьютерной техники, при этом в ходе производства следственных действий необходимо точно установить размер денежных средств, которые предполагалось похитить.

Целесообразным в данном случае будет дополнительное привлечение указанного лица к уголовной ответственности по ч. 2 ст. 349 УК «Несанкционированный доступ к компьютерной информации», так как описанные выше действия полностью соответствуют диспозиции указанной статьи, а под причинением существенного вреда можно понимать утрату конфиденциальности информации о размере и принадлежности банковского счета, причинение его законному владельцу морального вреда.

Подводя итог, отметим, что вопрос квалификации хищений, совершаемых с использованием банковских платежных карточек, имеет основополагающее значение в правоприменительной деятельности, так как во взаимосвязи с правильной правовой оценкой действий лиц, совершающих данные преступления, находится алгоритм действий следователя по расследованию дел рассматриваемой категории, который является базисным элементом криминалистического обеспечения расследования хищений, совершаемых с использованием банковских платежных карточек.

1. Воронцова, С.В. Проблемы безопасности электронных платежей, осуществляемых в международных платежных системах / С.В. Воронцова // Юрист. 2010. № 1.

2. Компьютерные преступления : рук. по борьбе с компьютер. преступлениям / Д. Айков [и др.]. М., 1999.

3. Крылова, В.В. Информационные компьютерные преступления : учеб. и практ. пособие / В.В. Крылова. М., 1997.

4. Лепехин, А.Н. Расследование преступлений против информационной безопасности: теоретико-правовые и прикладные аспекты : монография / А.Н. Лепехин. Минск, 2008.

5. О применении судами уголовного законодательства по делам о хищениях имущества : постановление пленума Верхов. суда Респ. Беларусь, 21 дек. 2001 г., № 15 // КонсультантПлюс : Беларусь [Электронный ресурс] / ООО «ЮрСпектр». Минск, 2013.

6. Об утверждении Инструкции о порядке совершения операций с банковскими платежными карточками : постановление правления Нац. банка Респ. Беларусь, 18 янв. 2013 г., № 34 // КонсультантПлюс : Беларусь [Электронный ресурс] / ООО «ЮрСпектр». Минск, 2013.

7. Петрухин, О.О. Виды мошенничества с использованием банковских пластиковых карточек / О.О. Петрухин // Вест. Акад. МВД Респ. Беларусь. 2005. № 2 (10). С. 130–134.

8. Расулев, А.К. Компьютерные преступления: уголовно-правовые и криминологические аспекты : автореф. дис. … канд. юрид. наук : 12.00.08 / А.К. Расулев. Ташкент, 2006.

9. Устьев, Л.Г. Уголовная ответственность за коррупционные информационные преступления : автореф. дис. … канд. юрид. наук : 12.00.08 / Л.Г. Устьев. Тамбов, 2010.

Дата поступления в редакцию: 24.04.13

***G.V. Glinsky**, investigator for particularly important cases of the investigation of crimes against the interests of the service department of the Investigative Committee of the Republic of Belarus in the Gomel region; **A.E. Nabatova**, PhD of law, associate professor, head of the department of management protection against emergencies of Gomel Engineering Institute of the Ministry of Emergency Situations of the Republic of Belarus*

ABOUT THE QUALIFICATION OF THEFT COMMITTED WITH THE USE OF BANK PAYMENT CARDS

The article deals with the problematic issues of qualification of theft committed with the use of bank cards. The authors determine the terms and definitions that are required for qualification of such crimes. The contentious issues arising in the legal assessment of the actions of the guilty are analyzed in terms of criminal law. The article considers legal practice case situation, the law enforcement procedures for their solution are proposed.

Keywords: crime, theft, bank cards, processing, processing center, authorization, theft, property funds.

УДК 343.98

***Е.Ю. Горошко**, кандидат юридических наук, старший преподаватель кафедры криминалистических экспертиз следственно-экспертного факультета Академии МВД Республики Беларусь*

ПОДГОТОВКА К ФОРМИРОВАНИЮ ЭКСПЕРТНОГО ПРОГНОЗА КАК ПРЕДВАРИТЕЛЬНАЯ СТАДИЯ МЕТОДИКИ ЭКСПЕРТНОГО ПРОГНОЗИРОВАНИЯ

Определяются основные требования, предъявляемые к методике экспертного прогнозирования, которые основываются на научных положениях социальной, криминологической и криминалистической прогностики. Предложено дифференцировать методику экспертного прогнозирования на три стадии, первой из которых является предварительная, рассмотрен ее содержательный аспект. Внимание уделено каждому этапу предварительной стадии методики экспертного прогнозирования, исследованы существующие позиции ученых в данной области.

Ключевые слова: прогноз, экспертное прогнозирование, методика формирования экспертных прогнозов, прогнозный фон, период упреждения прогноза, ретроспекция.

Методика формирования экспертных прогнозов в настоящее время является неразработанным методологическим элементом теории экспертного прогнозирования, что влечет малоэффективность, нерезультативность судебной экспертно-прогностической деятельности и, как следствие, снижает возможности профилактики и предотвращения преступлений.

В основе разработки научных положений методики экспертного прогнозирования, полагаем, лежат знания теории криминалистического прогнозирования, так как в настоящее время становление частной судебно-экспертной теории прогнозирования происходит путем отпочкования от теории криминалистической прогностики, закономерности развития и функционирования которой определяют фундаментальные основы формирующийся системы знаний.

Ученые-криминалисты в отношении методики разработки криминалистических прогнозов на протяжении многих лет высказывали разные мнения, но все они едины в одном: методика формирования прогноза – наиболее сложный раздел криминалистической прогностики. То же можно констатировать и в отношении методики экспертного прогнозирования.

В науке в отношении методики формирования прогноза существуют разные позиции. Так, Г.Л. Грановский отождествляет методику с методами прогнозирования [4, с. 39]. Р.С. Белкин включает в нее различные процедуры по сбору информации об объекте и тенденциях его развития, операции по прогнозированию, оценку и реализацию прогноза [2, с. 135].

Методика прогнозирования по своей сути является одним из основных элементов изучаемой теории, посредством которого реализуется ее практическое значение, поэтому отсутствие взаимопонимания у специалистов ведет к увеличению опасности разработки ошибочных прогнозов, негативные последствия от реализации которых нет необходимости доказывать. В силу сказанного целью настоящей статьи является рассмотрение имеющейся практики социального (общенаучного), криминологического и криминалистического прогнозирования и разработка единых научных основ методики экспертной прогностики.

Выбор указанных дисциплин базируется на том, что теория экспертного прогнозирования, как уже указывалось, отпочковалась от теории криминалистического прогнозирования, которая, в свою очередь, как разновидность правового прогнозирования отпочковалась от социальной прогностики, теоретический аппарат которой во многом определил содержание формирующейся в настоящее время частной судебно-экспертной теории.

Между методиками социального, криминологического, криминалистического и экспертного прогнозирования есть много общего. Однако в их содержании имеются и существенные различия, обусловленные главным образом особенностями объектов прогнозирования и статусом субъектов прогностической деятельности. Например, разработка прогноза характеристики прогнозируемого механизма преступления требует применения методов статистического анализа, моделирования. Прогнозирование динамики преступности в регионе предполагает использование математических методов, а прогнозы социальных процессов обычно разрабатываются по методу Дельфи [9].

Полагаем, за основу разработки общих начал методики экспертного прогнозирования нужно взять исследования, осуществленные в социальном прогнозировании, которые впоследствии использовались при разработке методики криминалистического прогнозирования. Во-первых, социальное прогнозирование является первоначальным в системе научного знания, предметом которого было изучение закономерностей прогностической деятельности. В настоящее время социальное прогнозирование за полу-