УДК 343.9.018.3
ББК 67.518.9

А.А. Чеботарева
кандидат юридических наук, доцент,
Московский государственный университет путей сообщения,
г. Москва, Российская Федерация

КОМПЬЮТЕРНАЯ ПРЕСТУПНОСТЬ В БАНКОВСКОЙ СФЕРЕ: ОСНОВНЫЕ НАПРАВЛЕНИЯ УГОЛОВНО-ПРАВОВОЙ ПОЛИТИКИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

В статье анализируется основное направление уголовно-правовой политики современной России – ужесточение уголовной ответственности за преступления в банковской сфере, совершаемые с использованием высоких технологий. Массовое использование платежных услуг в условиях подстегиваемого развитием высоких технологий увеличения опасности неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий в отношении информации выводит проблему преступности на новый уровень. Автор акцентирует внимание на особенностях компьютерных преступлений в банковской сфере, на вопросах противодействия им как на национальном, так и на международном уровне. Подчеркивается важность и своевременность предпринимаемых законодательных инициатив, направленных на ужесточение уголовной ответственности за преступления, совершаемые с использованием высоких технологий. Осознание степени общественной опасности преступлений в банковской сфере в условиях масштабности таких деяний как следствия стремительных процессов информатизации диктует необходимость реформирования действующего уголовного законодательства. Поднимаются проблемы предупреждения совершаемых преступных деяний, вопросы необходимости выработки системы мер борьбы с активным использованием в криминальных целях ресурсов Интернета. Также акцентируется внимание на международной информационной безопасности, необходимости решения вопроса унификации национального уголовного законодательства с международными нормами в области компьютерной преступности.

Ключевые слова: уголовно-правовая политика; информационное общество; динамика компьютерной преступности; информационная безопасность; транснациональная преступность; хищение; компьютерное мошенничество; хищение с использованием компьютерной техники.

A.A. Chebotareva
Candidate of Legal Sciences, Associated Professor,
Moscow State University of Railway Engeneering,
Moscow, Russian Federation

CYBER-CRIME IN BANKING SECTOR: RUSSIAN FEDERATION CRIMINAL POLICY MAIN DIRECTIONS

Abstract

The article analyses Russian Federation criminal policy main direction – enhancement of criminal penalty enhancement for high-tech cyber-crime in banking sector. Crime problem reached new level due to mass use of payment service in terms of high-tech development driven danger increase of illegal access, erasure, modification, blocking, copying, distribution of information and other unlawful actions. The author emphasizes aspects of cyber-crime in banking sector, its counteraction nationally and internationally and proves it really important to develop legislative initiatives aimed at penalty for high-tech crimes enhancement. Current criminal law has to be

reformed due to extreme social danger of crimes in banking sector determined by these crimes' scale and rapid IT penetration. The article raises problems of crime prevention and development of Internet-related crimes counteraction system. The author pays special attention to international information security issue, necessity for national and international criminal law unification in terms of cyber-crime.

Key words: criminal law; information society; cyber-crime dynamics; information security; international crime; fraud; cyber fraud; fraud with use of computer.

Информационное общество, т.е. общество, в котором информационные процессы осуществляются главным образом на основе использования информационно-коммуникационных технологий, а информационные ресурсы доступны всем слоям населения, переживает один из самых активных этапов своего развития. А значит, актуально все, что связано с понятием безопасности в условиях формирования электронного государства, с понятием информационной безопасности как всего государства в целом, общества, так и состояния защищенности в информационной среде каждой конкретной личности [4, с. 3; 5, с. 38].

Очевидные темпы роста количества правонарушений в виртуальном пространстве настораживают и свидетельствуют о необходимости адекватного правового реагирования. Внедрение информационных технологий осуществляется поэтапно, и развитие этого процесса в различных сферах происходило и происходит разными темпами. Так, одной из наиболее очевидных, динамичных на протяжении нескольких лет была информатизация банковской сферы. Итог – статистически подтверждаемый рост числа правонарушений / преступлений, связанных с причинением ущерба как гражданам, так и организациям в результате использования глобальных компьютерных сетей. Динамика совершаемых преступлений стремительна. По данным МВД России, в 2011 г. было выявлено 3 411 преступлений, предусмотренных ст. 187 Уголовного кодекса, в 2012 г. – 3 618, а только в первом полугодии 2013 г. – 3 013 (!).

Сложности анализируемого явления многоаспектны, одна из них – транснациональный характер киберпреступности в целом, что в условиях правонарушений в банковской сфере еще более угрожает безопасности как отдельной личности, так и общества и государства в целом. Банковская система как важнейший элемент финансово-кредитной сферы в условиях глобальной информатизации наиболее подвержена опасности хищений. А хищение денежных средств со счета клиента банка посредством компьютерных технологий не только касается защиты законных интересов отдельного клиента, но и затрагивает безопасность государства в кредитно-финансовой и бюджетной сфере, выявляет слабые звенья в противодействии посягательствам на совершение преступления в сфере охраняемой законом компьютерной информации, что может привести к дестабилизации как бюджетной, так и национальной платежной системы Российской Федерации. В связи с этим актуализируется научный интерес по ряду направлений: вопрос специфики хищений в банковской сфере с использованием высоких технологий, внимание к субъекту данных преступлений, исследование обстоятельств совершения преступных деяний в банковской сфере с использованием высоких технологий, проблема предупреждения таких преступлений, необходимость обобщения соответствующей следственной и судебной практики, выработка обоснованных предложений по совершенствованию действующего уголовного законодательства.

Безусловно, существенное значение в создании действенного механизма противодействия преступности имеет последовательность проводимой государством уголовно-правовой политики. Уголовно-правовая политика, являясь системообразующим элементом правовой политики государства, направлена на достижение стратегической цели, предусматривающей формирование нормативно-правовой основы, обеспечивающей надлежащую охрану законных прав личности, общества и государства от преступных посягательств и решение задач, связанных с реализацией мер по уменьшению и устранению преступности [1, с. 21].

Очевидно, что преступлениям, совершаемым в банковской сфере с использованием высоких технологий, присущи явные особен-

ности. Так, согласимся, что при совершении хищения с использованием компьютерной техники можно говорить о том, что применяется новая совокупность приемов, методов, последовательность действий, которая придает преступлению уникальные свойства, нехарактерные для других имущественных преступлений [3, с. 27].

Можно выделить ряд специфических черт преступных деяний в банковской сфере с использованием высоких технологий:

– это преступления, совершаемые с использованием компьютерной техники, компьютерных сетей;

– как следствие, совершаются они с помощью уникальных средств, повышающих общественную опасность содеянного;

– характеризуются высокой латентностью;

– такие преступления совершаются с корыстной целью, умышленно;

– степень общественной опасности этих преступлений высока;

– как правило, анализируемая преступность имеет характер организованной.

В современных условиях состояния преступности в банковской сфере, связанной с использованием высоких технологий, ужесточение уголовной ответственности – наиболее адекватный и обоснованный шаг. В связи с этим внесение в Государственную Думу РФ разработанного МВД России законопроекта об усилении уголовной ответственности на хищения в банковской сфере с использованием высоких технологий своевременно. Проект Федерального закона «О внесении изменений в статьи 187 и 272 Уголовного кодекса Российской Федерации» рассмотрен и одобрен на заседании Правительства Российской Федерации 15 мая 2014 г. и распоряжением от 30 мая 2014 г. № 921-р передан на рассмотрение нижней палатой парламента.

Представленным законопроектом подчеркивается прежде всего степень общественной опасности данных преступлений. Речь идет о преступлениях:

– против собственности, а именно о преступлениях в сфере экономической деятельности;

– против общественной безопасности и общественного порядка, в частности о преступлениях в сфере компьютерной информации.

В первом случае внимание акцентировано на ч. 1. ст. 187 УК РФ – законопроектом предлагается новая редакция диспозиции: «Изготовление в целях сбыта и (или) сбыт поддельных платежных карт, распоряжений о переводе денежных средств, документов или средств оплаты (за исключением случаев, предусмотренных статьей 186 Уголовного кодекса), а также электронных средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств…» Содержание диспозиции данной статьи в действующем уголовном законе более усеченное: «Изготовление в целях сбыта или сбыт поддельных кредитных либо расчетных карт, а также иных платежных документов, не являющихся ценными бумагами…» Расширенная, конкретизированная редакция диспозиции призвана поспособствовать как предупреждению совершения преступлений, так и эффективности борьбы с преступными деяниями в банковской сфере.

Проанализируем основные понятия новой редакции диспозиции ст. 187 УК РФ. Платежные карты – это инструмент безналичных расчетов, предназначенный для совершения физическими лицами, в том числе уполномоченными юридическими лицами (держателями), операций с денежными средствами, находящимися у эмитента (кредитной организации), в соответствии с законодательством Российской Федерации и договором с эмитентом. Под переводом денежных средств, согласно ст. 3 Федерального закона РФ от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе», понимаются действия оператора по переводу денежных средств в рамках применяемых форм безналичных расчетов по предоставлению получателю средств денежных средств плательщика. Электронное средство платежа законодатель в том же законе определяет как средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических средств.

Проектом Федерального закона «О внесении изменений в статьи 187 и 272 Уголовного

кодекса Российской Федерации» меры наказания, установленные за совершение одного из наиболее распространенных компьютерных преступлений – неправомерный доступ к компьютерной информации (ч. 2 ст. 272 УК РФ), приводятся в соответствие со степенью общественной опасности. Согласно нормам действующего законодательства, лишение свободы за неправомерный доступ к компьютерной информации с причинением крупного ущерба или же совершение такого деяния из корыстной заинтересованности составляет шесть месяцев. Законопроектом же максимальный срок увеличивается до четырех лет.

В сложившейся ситуации резкого увеличения количества преступных деяний в банковской сфере с использованием высоких технологий абсолютно обоснованна необходимость, в целях защиты законных прав и интересов отдельной личности, юридических лиц, общества, государства в целом, ужесточения уголовной ответственности в отношении таких деяний. Это обусловлено объективными факторами, определяющими опасность деяния и его последствий. Требует своего грамотного решения проблема предупреждения совершаемых преступных деяний в сфере компьютерной информации, выработки эффективной системы мер борьбы с активным использованием в криминальных целях ресурсов Интернета.

Учет транснационального характера преступлений в банковской сфере с использованием высоких технологий выводит в ряд актуальных вопросов и проблему унификации национального уголовного законодательства с международными нормами в области компьютерной преступности. Речь идет о международной информационной безопасности. Согласно Основам государственной политики РФ в области международной информационной безопасности на период до 2020 года, это такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры.

Согласимся, что сегодня в России на повестке дня стоит вопрос о создании новых органов и организаций, координирующих и осуществляющих борьбу с киберпреступностью, что, в свою очередь, требует подготовки национальных кадров, представителей которых можно было бы привлекать на службу в транснациональные органы и организации, направленные на борьбу с киберпреступностью [2, с. 33]. Ввиду неминуемого ежегодного прироста числа таких преступлений необходимо также обратить серьезнейшее внимание на вопросы обучения основам информационной безопасности, информационных технологий представителей судебной системы и правоохранительных органов. Как вышеназванные, так и другие обоснованные шаги в направлении совершенствования уголовно-правовой политики государства по отношению к преступлениям в банковской сфере с использованием высоких технологий позволят создать эффективную систему информационной безопасности в таком важном элементе финансово-кредитной сферы, как банковская система. Динамично растущая преступность в этом секторе экономики должна порождать новые, соответствующие меры борьбы с нею.

ПРИСТАТЕЙНЫЙ СПИСОК ЛИТЕРАТУРЫ

1. Авдеев В.А. Концепция уголовно-правовой политики Российской Федерации: основные направления совершенствования уголовного закона и оптимизации мер противодействия преступности / В.А. Авдеев, О.А. Авдеева // Криминологический журнал Байкальского государственного университета экономики и права. – 2014. – № 1. – С. 12–24.

2. Протасевич А.А. Борьба с киберпреступностью как актуальная задача современной науки / А.А. Протасевич, Л.П. Зверянская // Криминологический журнал Байкальского государственного университета экономики и права. – 2011. – № 3. – С. 28–33.

3. Хилюта В.В. Необходимость установления уголовной ответственности за хищения, совершаемые с использованием компьютерной техники / В.В. Хилюта // Криминологический журнал Байкальского государственного университета экономики и права. – 2012. – № 1. – С. 26–31.

4. Чеботарева А.А. Научные подходы к определению понятия «информационная безопасность» / А.А. Чеботарева // Информационное право. – 2011. – № 1. – С. 3–6.

5. Чеботарева А.А. Теоретико-правовое исследование понятия «информационная безопасность личности» / А.А. Чеботарева // Юридический мир. – 2010. – № 6. – С. 38–41.

REFERENCES

1. Avdeev V.A., Avdeeva O.A. Criminal legal policy concept of the Russian Federation: main directions of criminallaw improvement and crime counteraction measures optimization. [Avdeev V.A., Avdeeva O.A. Koncepcija ugolovno-pravovoj politiki Rossijskoj Federacii: osnovnye napravlenija sovershenstvovanija ugolovnogo zakona i optimizacii mer protivodejstvija prestupnosti]. *Kriminologicheskij zhurnal Bajkal'skogo gosudarstvennogo universiteta jekonomiki i prava – Criminology Journal of Baikal National University of Economics and Law*, 2014, no. 1, pp. 12–24.
2. Protasevich A.A., Zverjanskaja L.P. Fighting cybercrimes as an urgent task for contemporary research [Protasevich A.A., Zverjanskaja L.P. Bor'ba s kiberprestupnost'ju kak aktual'naja zadacha sovremennoj nauki]. *Kriminologicheskij zhurnal Bajkal'skogo gosudarstvennogo universiteta jekonomiki i prava – Criminology Journal of Baikal National University of Economics and Law*, 2011, no. 3, pp. 28–33.
3. Hiljuta V.V. The necessity of establishing criminal liability for larceny committed with the aid of computer equipment [Hiljuta V.V. Neobhodimost' ustanovlenija ugolovnoj otvetstvennosti za hishhenija, sovershaemye s icpol'zovaniem komp'juternoj tehniki]. *Kriminologicheskij zhurnal Bajkal'skogo gosudarstvennogo universiteta jekonomiki i prava – Criminology Journal of Baikal National University of Economics and Law*, 2012, no. 1, pp. 26–31.
4. Chebotareva A.A. Scientific approaches to «informational security» term definition. [Chebotareva A.A. Nauchnye podhody k opredeleniju ponjatija «informacionnaja bezopasnost'»]. *Informacionnoe pravo – Informational law*, 2011, no. 1, pp. 3–6.
5. Chebotareva A.A. Theoretical and legal research of «personal informational security» term. [Chebotareva A.A. Teoretiko-pravovoe issledovanie ponjatija «informacionnaja bezopasnost' lichnosti»]. *Juridicheskij mir – Legal law*, 2010, no. 6, pp. 38–41.

Сведения об авторе

Чеботарева Анна Александровна – доцент юридического института Московского государственного университета путей сообщения, кандидат юридических наук, доцент, г. Москва, Российская Федерация; e-mail: anna_galitskaya@mail.ru.

Information about author

Chebotareva Anna Aleksandrovna – Associated Professor of Law institute of Moscow State University of Railway Engeneering, Candidate of Legal Sciences, Associated Professor, Moscow, Russian Federation; e-mail: anna_galitskaya@mail.ru.