ПРЕСТУПЛЕНИЯ В СФЕРЕ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ В СИСТЕМЕ ЭКОНОМИЧЕСКОЙ ПРЕСТУПНОСТИ

В. А. Миклашевская

Белорусский государственный университет, г. Минск,
violetta.miklashevskaya@gmail.com
науч. рук. – Г. А. Шумак, канд. юрид. наук, доцент

В настоящей работе исследуются преступные деяния в сфере банковской деятельности. Отмечен значительный рост преступлений в сфере банковской деятельности с использованием компьютерной техники и технологий в Республике Беларусь. Проведено обобщение противоправных деяний, связанных со злоупотреблением возможностями новейших электронных систем и коммуникационных средств, в результате которого были выделены несколько групп. Выявлен опыт зарубежных стран в законодательном регулировании названного вида преступных деяний. В ходе анализа исследуемой темы были определены наиболее распространенные способы совершения хищений с использованием компьютерной техники. Систематизированы различия между такими видами преступлений, как хищение с использованием компьютерной техники и кража, мошенничество.

Ключевые слова: экономическая преступность; банковские преступления; компьютерные преступления; мошенничество; киберхищения.

Наиболее опасные проявления экономической преступности в связи с активным ростом роли финансов и кредита представлены в сфере банковской деятельности.

Интерес к совершению противоправных деяний в сфере банковской деятельности начал возрастать лишь с начала 1950-х гг.

Кроме того, динамичное внедрение новейших электронных систем и коммуникационных средств в различные сферы деятельности современного общества привело как к развитию положительных тенденций, так и тенденций негативного характера.

Условно противоправные деяния, связанные со злоупотреблением возможностями компьютерной техники, могут быть разделены на несколько групп:

- преступления, направленные на незаконное завладение, изъятие, уничтожение либо повреждение средств компьютерной техники и носителей информации как таковых;
- преступления, направленные на получение несанкционированного доступа к компьютерной информации, ее модификации, связанные с неправомерным завладением компьютерной информацией, разработкой, использованием либо распространением вредоносных программ и т.д., т.е. компьютерная информация является объектом преступного посягательства;

• преступления, в которых компьютеры и другие средства компьютерной техники используются в качестве орудия или средства совершения корыстного преступления, и умысел виновного лица направлен на завладение чужим имуществом путем изменения информации либо путем введения в компьютерную систему ложной информации [2, с. 32].

Следует отметить, что основная масса компьютерных преступлений в Соединенных Штатах Америки (далее – США), Федеративной Республике Германия (далее – ФРГ) и других государствах совершается с использованием всемирной компьютерной сети Интернет, характеризующейся активным ростом криминальных проявлений.

Так, уголовное законодательство США, посвященное борьбе с преступлениями с использованием компьютерной техники и технологий, отличается своеобразием и постоянным обновлением. Основной закон США, касающийся компьютерных преступлений, был сформулирован в 1986 г. «О мошенничестве и злоупотреблениях, связанных с компьютерами», а впоследствии состав «мошенничества с использованием компьютеров» вошел в Свод законов США. В параграфе 1030 (a) (4) Свода законов США мошенничество с использованием компьютера определяется как доступ, осуществляемый с мошенническими намерениями, и использование компьютера с целью получения чего бы то ни было ценного посредством мошенничества, включая незаконное использование машинного времени (то есть бесплатное использование компьютерных сетей и серверов) стоимостью более пяти тысяч долларов США в течение года, то есть без оплаты использования компьютерных сетей и серверов [3, с. 31].

Ответственности за компьютерное мошенничество согласно параграфу 263a Уголовного кодекса ФРГ (далее – УК ФРГ) подлежит лицо, которое «действуя с намерением получить для себя или третьего лица имущественную выгоду, причиняет вред имуществу другого лица, воздействуя на результат обработки данных путем неправильного создания программ, использования неправильных или неполных данных, путем неправомочного использования данных или иного неправомочного воздействия на процесс обработки данных». В данном случае компьютер используется как орудие совершения преступления, поскольку указанные в параграфе 263a УК ФРГ формы реализации объективной стороны выступают именно в качестве способов достижения корыстной цели. Таким образом, немецкий законодатель четко разграничил два вида мошенничества: традиционное и компьютерное. Суть же компьютерного мошенничества заключается в том, что обману подвергается не человек, а программа, поскольку ущерб имуществу причиняется воздействием на процесс переработки информации и путем неправильного установления

программы, использования неверных или неполных данных, а также путем неправомочного использования данных или неправомочного воздействия на процессы переработки данных.

Следует обратить внимание на значительный рост в Республике Беларусь преступлений в сфере банковской деятельности, связанных с использованием электронных средств доступа к информации (компьютерные, телекоммуникационные системы, кредитные карточки и другие).

Такой вид хищений характеризуется тем, что преступники, воспользовавшись служебной возможностью для неправомерного доступа к компьютерной информации финансового характера, сосредоточенной в вычислительных (расчетных) центрах банковских учреждений, и обнаружив пробелы в деятельности таких учреждений, осуществляют различные незаконные операции с указанной информацией в целях хищения денежных средств. Наиболее широкое распространение в последнее время получили следующие способы совершения хищений с использованием компьютерной техники:

- тайное введение в чужое программное обеспечение специально созданных программ, которые, попадая в информационно-вычислительные системы (обычно выдавая себя за известные сервисные программы), начинают выполнять новые, не планировавшиеся законным владельцем программы с одновременным сохранением прежней работоспособности системы;
- изменение или введение в компьютерную систему данных при вводе-выводе информации, в результате чего, например, происходит модификация данных в автоматизированной системе банковских операций;
- введение в прикладное программное обеспечение банковской компьютерной системы специальных программных модулей, обеспечивающих отчисление на заранее открытый подставной счет мелких денежных сумм с каждой банковской операции или увеличение суммы на этом счете при автоматическом пересчете рублевых остатков;
- установление кода компьютерного проникновения в электронную платежную сеть расчетов по пластиковым карточкам (путем несанкционированного доступа к банковским базам данных посредством телекоммуникационных сетей) и создание двойников банковских пластиковых карточек с последующим хищением денежных средств;
- проведение фиктивных платежей по системе межбанковских электронных расчетов путем внесения изменений в алгоритмы обработки электронных данных [4, с. 136].

Необходимо указать, что хищение с использованием компьютерной техники имеет определенные сходства с кражей и мошенничеством. Од-

нако, главным различием указанных противоправных деяний является тот факт, что при хищении с использованием компьютерной техники такое деяние осуществляется путем информационного воздействия на компьютерную систему, которая принимает решение о совершении тех или иных операций. В связи с этим при квалификации хищений, совершаемых с использованием компьютерной техники, должны учитываться не составные элементы этой самой техники и даже не всегда ее использование, поскольку использование компьютерной техники может выступать как средство для совершения хищения, а воздействие на результат автоматизированной обработки данных в целях завладения чужим имуществом.

Именно на данное обстоятельство обращается внимание в постановлении Пленума Верховного Суда Республики Беларусь от 21 декабря 2001 г. № 15 «О применении судами уголовного законодательства по делам о хищениях имущества», в пункте 20 которого разъясняется о том, что «хищение путем использования компьютерной техники (статья 212 УК) возможно лишь посредством компьютерных манипуляций, заключающихся в обмане потерпевшего или лица, которому имущество вверено или под охраной которого оно находится, с использованием системы обработки информации. Данное хищение может быть совершено как путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, так и путем введения в компьютерную систему ложной информации» [1].

Таким образом, в результате исследования был отмечен значительный рост в Республике Беларусь преступлений в сфере банковской деятельности, связанных с использованием компьютерной техники и технологии в связи с активным развитием информационных и компьютерных технологий в Республике Беларусь.

Библиографические ссылки

1. О применении судами уголовного законодательства по делам о хищениях имущества [Электронный ресурс] : постановление Пленума Верховного Суда Республики Беларусь, 21 дек. 2001 г., № 15 : в ред. постановления Пленума Верховного Суда Респ. Беларусь от 31.03.2016 // КонсультантПлюс. Беларусь / ООО «ЮрСпектр» / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.
2. *Гончаров Д. Ю.* Квалификация хищений, совершаемых с помощью компьютеров // Законность. 2001. № 11. С. 31–33.
3. *Громов Е. В.* Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах // Вестник ТГПУ. 2006. № 11. С. 31–32.
4. *Шумак Г. А.* Криминалистический анализ должностных хищений // Право и демократия. Межвуз. сб. науч. тр. 1990. № 3. С. 136–145.