УДК 343.3/7

А.К. Раев, магистр юридических наук, старший преподаватель-методист, майор полиции Алматинской академии МВД Республики Казахстан им. М. Есбулатова
mvdas88@gmail.com

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ В УГОЛОВНОМ ЗАКОНОДАТЕЛЬСТВЕ РЕСПУБЛИКИ КАЗАХСТАН

Основной причиной возникновения компьютерной преступности априори можно назвать возникновение и быстрое развитие самих информационных технологий. Иначе говоря, до XX в. компьютерные преступления не регистрировались именно в силу объективной невозможности их совершения, отсутствия компьютеров и компьютерных технологий.

Современное развитие кибериндустрии способствует созданию самых различных инструментов, используемых для совершения компьютерных преступлений. При этом все компьютерные преступления, на наш взгляд, можно разделить на две основные группы.

Первая группа охватывает преступные деяния, совершаемые с помощью современных технологий, позволяющих посредством информационно-коммуникационных сетей совершить любое преступное деяние, не исключая даже убийство. Так, широкую известность получил случай из практики США, где раненый при покушении свидетель, находящийся под программой государственной защиты, был помещен в охраняемую палату в больнице. Преступники смогли довести до конца свой замысел на убийство свидетеля путем изменения компьютерной программы прибора стимуляции сердца, незаконно подключившись к сети Интернет больницы. Еще большее распространение получили преступления против собственности (кражи со счетов, интернет-мошенничества и др.), совершаемые с применением компьютеров. Такие деяния отличаются от классических преступлений лишь использованием компьютерных технологий в качестве орудий совершения преступления.

Вторая группа компьютерных преступлений – преступные деяния, совершаемые непосредственно внутри информационно-коммуникационной сферы (действия хакеров, взломщиков, Doc-злоумышленников и др.). Эти компьютерные преступления непосредственно посягают на безопасность информационных сетей.

Следует отметить, что в Уголовном кодексе Республики Казахстан (УК РК) 2014 г. предусмотрена специальная гл. 7 «Уголовные правонарушения в сфере информатизации и связи», в которую включены составы преступлений, непосредственно связанных с информационными правоотношениями, т. е. деятельностью с информацией как самостоятельным объектом.

Развитие информационных сетей и само создание глобальной компьютерной сети Интернет во многом расширило обычные границы представлений и деятельности человека, при этом реалии менялись столь стремительно, что сфера законодательства не успевала их охватить – это появление принципиально новых технологий, новых угроз безопасности, новых видов и новых способов и средств совершения преступных деяний.

Необходимо осознавать при этом всю сложность проблем, с которыми пришлось столкнуться отечественным законодателям при формировании такой новой подотрасли права, как информационное право. Прежде всего это отсутствие единого подхода в выборе и использовании терминов в данной сфере. Мнения теоретиков достаточно сильно различаются даже по поводу самого понятия «информация» в праве.

Терминологическая неопределенность повлекла за собой неопределенность в определении объектов информационных отношений как объектов правовой охраны. Кроме того, сложность рассматриваемой сферы правоотношений требует от законодателя и правоприменителей достаточно высокой квалификации и наличия определенного уровня знаний в области информационно-технической деятельности.

Исходя из вышеизложенного можно говорить о возникновении относительно обособленной группы общественных отношений – информационных отношений, выделяемых по признаку информации как объекта этих отношений. Действия субъектов права, связанные с созданием, передачей, обменом, хранением, потреблением, распространением и иным оборотом информации, информационных ресурсов, – основные объекты правового регулирования, которые могут и должны быть урегулированы правом. Следовательно, можно вести речь о формировании новой комплексной отрасли права – информационного права.

Вопрос о существовании данной отрасли сам по себе является спорным. В Российской Федерации такая отрасль включена в номенклатуру специальностей научных работников. В Республике Беларусь информационное право также признано самостоятельной отраслью науки, по которой присуждаются ученые степени (12.00.13). В Казахстане в правовых специальностях такого направления пока не предусмотрено.

Полагаем, что выделение информационного права как самостоятельной отрасли правовой науки полностью обоснованно. Прежде всего это подтверждается наличием информационных отношений как самостоя-

тельного предмета правового регулирования. Информационные правоотношения связаны с компьютерными процессами сбора, создания, обработки, распространения информации, направленными на решение информационных запросов граждан, организаций, общества и государства. Учитывая, что разнообразие существующих информационных отношений актуализирует вопрос об обеспечении информационной безопасности, правовое регулирование этих отношений, определение возможных деликтов и установление мер юридической ответственности за их совершение представляется логичным и необходимым шагом.

Важный момент заключается в том, что сегодня от уровня эффективности использования информации зависит общий уровень развития государства, обеспечения безопасности общества и граждан. Охраняемая нормами уголовного права информация – лишь небольшая часть всех информационных ресурсов. Постоянное увеличение как количества, так и видов преступлений в сфере информации диктует необходимость уточнения объективной стороны составов соответствующих уголовных правонарушений, а также дифференциации уголовной ответственности виновных лиц. Полагаем, не подлежит сомнению неизбежность будущих изменений уголовного закона в части информационных уголовных правонарушений.

УДК 004:343

Н.И. Рудович, кандидат юридических наук, доцент учреждения образования «Белорусский государственный экономический университет»
Roodnik@mail.ru;
Е.О. Ковалёва, студентка учреждения образования «Белорусский государственный экономический университет»
Katia.10.12.2000@gmail.com

СОВЕРШЕНСТВОВАНИЕ МЕХАНИЗМОВ ЗАЩИТЫ ПОРЯДКА ПРОВЕДЕНИЯ ЭЛЕКТРОННЫХ РАСЧЕТОВ

Система «Home Banking» получила широкое распространение в 80-х гг. прошлого столетия в США. Основная задача данной системы – обеспечение технической возможности клиентам банка контролировать свои счета. С развитием информационных технологий и расширением спектра оказываемых услуг банками своим клиентам была предложена дополнительная функция перевода денежных средств. Благодаря своей многофункциональности и удобству использования, система «Home Banking» приобрела широкое распространение за пределами США.

В странах постсоветского пространства данная система стала использоваться в гражданском обороте в конце 1990-х гг. Несмотря на некоторые трудности ее внедрения в банковском секторе, можно говорить о том, что сегодня онлайн-банкинг имеет повсеместное использование в различных сферах деятельности граждан указанных государств.

Доступность и удобство использования онлайн-банкинга в современных условиях привлекает множество клиентов, и, вполне очевидно, что в вопросах онлайн-расчетов на первое место выходит их безопасность. Интернет-банкинг предоставляет возможность беспроблемного доступа к использованию банковской платежной карточки: чтобы провести операцию необходимо иметь доступ в онлайн-банк и соответствующие пароли. Следовательно, основной задачей участников расчетных отношений в таких случаях становится обеспечение безопасности личного кабинета.

Актуальность обеспечения безопасности данной формы расчетов обусловлена частыми случаями несанкционированного доступа к средствам клиентов на счетах. Специалисты в сфере противодействия преступлениям, совершенным с использованием высоких технологий, выделяют несколько основных причин угрозы безопасности. Так, текущей основной проблемой безопасности данных в Интернет-банкинге является фишинг. Злоумышленники, представляясь официальной организацией, рассылают ложные сообщения клиентам с просьбой сообщить личные данные. Телефонный «фишинг» работает аналогично обычному, только в этом случае клиенту поступают звонки от лжепредставителей банка. Возможно также похищение баз данных в самом банке. В таком случае злоумышленник может получить доступ к множеству счетов клиентов. Как правило, в подобных случаях убытки полностью возмещаются самим банком, не дожидаясь поимки мошенников. Достаточно распространенная схема получения паролей и логинов путем внедрения различных вирусных программ, которые могут устанавливаться как на компьютеры, так и на телефоны или планшеты.

Широкое распространение в электронных расчетах параллельно компьютерному онлайн-банкингу получили мобильные приложения для смартфонов и планшетов. Они достаточно эффективны и удобны в использовании, а по функционалу мало отличаются от компьютерного онлайн-банка. Однако, как отмечают специалисты, в случае входа в Интернет-банк через мобильное устройство риск взлома персональных данных в разы увеличивается.

Среди основных методов защиты данных от противоправного проникновения со стороны третьих лиц наибольшее распространение получило шифрование данных. Банки, предоставляющие услугу Интернет-банкинга, применяют SSL-шифрование данных, передаваемых от