ISSN 2500-4255

УДК 343.97
DOI 10.17150/2500-4255.2017.11(1).13-21

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ЭКОНОМИКИ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

А.П. Суходолов[1], С.В. Иванцов[2], С.В. Борисов[3], Б.А. Спасенников[4]
[1] Байкальский государственный университет, г. Иркутск, Российская Федерация
[2] Московский университет МВД России им. В.Я. Кикотя, г. Москва, Российская Федерация
[3] Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, г. Москва, Российская Федерация
[4] Научно-исследовательский институт Федеральной службы исполнения наказаний России, г. Москва, Российская Федерация

Информация о статье

Дата поступления
2 февраля 2017 г.

Дата принятия в печать
21 февраля 2017 г.

Дата онлайн-размещения
28 марта 2017 г.

Ключевые слова
Цифровая экономика; киберпреступность; криминология; предупреждение преступлений в сфере экономики; профилактика преступного поведения; информационная безопасность; информационно-телекоммуникационные сети; экономическая безопасность

Аннотация. Цель выполненного исследования заключалась в выделении и изучении современных проблем противодействия преступности в сфере экономики, связанных с особенностями совершения соответствующих уголовно наказуемых деяний с использованием возможностей информационно-телекоммуникационных сетей, прежде всего сети Интернет, для формирования предложений по оптимизации системы предупреждения таких преступлений. В работе применялись общенаучные и частные научные методы с превалированием социологических методов исследования. На основе специально разработанных анкет авторами было опрошено 78 судей, 126 сотрудников правоохранительных органов и 95 научно-педагогических работников относительно проблем предупреждения указанных преступлений и предложений по их минимизации. Также были проанализированы материалы 120 уголовных дел о преступлениях данной группы, изучена опубликованная практика Верховного Суда Российской Федерации. Выявлено, что нарастание проблем в области предупреждения экономической преступности усугубляется непрерывным увеличением числа новых способов совершения соответствующих деяний. Использование информационно-телекоммуникационных сетей, в первую очередь сети Интернет, становится одним из основных способов совершения ряда преступлений в сфере экономической деятельности. Прогнозируется тенденция к повышению доли экономических преступлений, совершаемых таким способом. Особенности данного способа связаны с техническими возможностями, предоставляемыми информационными технологиями, обеспечивающими удаленность действий виновных лиц от места наступления последствий преступления, с относительной анонимностью данной криминальной деятельности и ее транснациональным характером. Наиболее востребована профилактика таких преступлений и активизация международного сотрудничества в области их предупреждения. На основе изучения выделенных проблем авторы предлагают свое видение формирования системы предупреждения преступлений в сфере экономики, совершаемых с использованием информационно-телекоммуникационных сетей, в том числе касающееся совершенствования законодательства в данной области.

TOPICAL ISSUES OF PREVENTING ECONOMIC CRIMES COMMITTED WITH THE USE OF INFORMATION AND TELECOMMUNICATION NETWORKS

Alexander P. Sukhodolov[1], Sergey V. Ivantsov[2], Sergey V. Borisov[3], Boris A. Spasennikov[4]
[1] Baikal State University, Irkutsk, the Russian Federation
[2] V.Ya. Kikotya Moscow University of the Ministry of Internal Affairs of Russia, Moscow, the Russian Federation
[3] Institute of Legislation and Comparative Law of the Government of the Russian Federation, Moscow, the Russian Federation
[4] Research Institute of Federal Penitentiary Service of Russia, Moscow, the Russian Federation

Article info

Received
2017 February 2

Accepted
2017 February 21

Abstract. The goal of this research is to identify and study contemporary issues of counteracting economic crimes connected with the specific character of these offences — the use of information and telecommunication networks, primarily, the Internet, and to present ideas on optimizing the system of such crimes' prevention. The authors used general and specific research methods, sociology methods being the dominant ones. The authors designed special questionnaires to survey 78 judges, 126 law enforcement employees and 95 professionals working in research and education on the prevention

ISSN 2500-4255

Available online
2017 March 28

Keywords
Digital economy; cybercrime; criminology; prevention of economic crimes; prevention of criminal behavior; information security; information and telecommunication networks; economic security

of the above-mentioned crimes and the ideas on their minimization. They also analyzed 120 criminal cases of this type and researched the published materials of the Supreme Court of the Russian Federation. The authors found out that increasing difficulties in the sphere of economic crimes' prevention are aggravated by a steady growth in the number of new ways of committing them. The use of information and telecommunication networks, primarily, the Internet, becomes one of the dominant methods of committing a number of economic crimes. The authors predict a trend for the growth of the share of economic crimes committed this way. The specific features of this crime method are connected with technological opportunities provided by information technologies, where the guilty party is distanced from the crime scene; this criminal activity is relatively anonymous and has a transnational character. The prevention of such crimes and the activization of international cooperation in their prevention are very much demanded. Conducted research allowed the authors to present their own vision of establishing a system for the prevention of economic crimes committed with the use of information and telecommunication networks, including the improvement of relevant legislation.

Защищенность экономических отношений от кибератак и иных противоправных действий, совершаемых с использованием информационно-телекоммуникационных сетей, в первую очередь сети Интернет, беспокоит все мировое сообщество [1–4]. На 13-м Конгрессе ООН по предупреждению преступности и уголовному правосудию, состоявшемся в 2015 г.[1], посвященном преимущественно противодействию транснациональному криминалитету, была, в частности, подчеркнута необходимость обеспечения использования экономических, социальных и технологических благ в качестве положительной силы, помогающей странам развивать сотрудничество в сфере предупреждения новых и возникающих форм преступности и борьбы с ними. Для этого предлагается разрабатывать и осуществлять всеобъемлющие меры реагирования в области предупреждения преступности и уголовного правосудия, в том числе принимать необходимые законодательные и административные меры для эффективного предупреждения новых, появляющихся и видоизменяющихся форм преступности и борьбы с ними на региональном, национальном и международном уровнях.

Применительно к киберпреступности было предложено опробовать конкретные меры по созданию защищенной и устойчивой киберсреды, предупреждать и пресекать преступную деятельность, осуществляемую с использованием сети Интернет, развивать сотрудничество между правоохранительными органами на национальном и международном уровнях, повышать защищенность компьютерных сетей и обеспечивать защиту соответствующей инфраструктуры, стараться оказывать долгосрочную техническую помощь и содействие национальным ведомствам в наращивании их потенциала в области противодействия киберпреступности, в том числе посредством профилактики, выявления, расследования и уголовного преследования таких преступлений во всех их формах.

В Стратегии национальной безопасности Российской Федерации[2] к числу главных стратегических угроз национальной безопасности в области экономики отнесены, в частности, незащищенность национальной финансовой системы от действий нерезидентов, уязвимость ее информационной инфраструктуры, сохранение значительной доли теневой экономики и условий для криминализации хозяйственно-финансовых отношений. При этом отмечается появление новых форм противоправной деятельности, осуществляемой с использованием информационных, коммуникационных и высоких технологий.

В Доктрине информационной безопасности Российской Федерации[3] указано, что информационные технологии с течением времени приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства, поэто-

[1] Проект Дохийской декларации о включении вопросов предупреждения преступности и уголовного правосудия в более широкую повестку дня Организации Объединенных Наций в целях решения социальных и экономических проблем и содействия обеспечению верховенства права на национальном и международном уровнях, а также участию общественности [Электронный ресурс] : принят на 13-м Конгр. ООН по предупреждению преступности и уголов. правосудию, Доха, 12–19 апр. 2015 г. URL: http://crimescience.ru/?p=542.

[2] О стратегии национальной безопасности Российской Федерации : указ Президента РФ от 31 дек. 2015 г. № 683 // Собрание законодательства РФ. 2016. № 1, ч. 2. Ст. 212.

[3] Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента РФ от 5 дек. 2016 г. № 646 // Там же. № 50. Ст. 7074.

му их эффективное применение следует рассматривать как фактор ускорения экономического развития государства и формирования информационного общества. Вместе с тем, как подчеркивается в данном документе, наблюдается рост компьютерной преступности, прежде всего в кредитно-финансовой сфере, причем способы и средства совершения таких преступлений становятся все изощреннее.

Отметим, что в последние годы российские ученые стали обращать пристальное внимание на активизацию использования информационно-телекоммуникационных сетей для совершения различных преступлений, в том числе относящихся к числу экономических, террористических и экстремистских уголовно наказуемых деяний [1; 5; 6]. Вместе с тем специализированные научные исследования в данной области проводятся редко и, как правило, имеют узкую направленность, тогда как выделенная проблема отличается комплексным характером и требует системного подхода к ее решению. Национальный законодатель также с запозданием реагирует на видоизменения преступности, в том числе на новые способы совершения преступлений в сфере экономики, обусловленные развитием информационных технологий [2; 6].

Анализ норм разд. VIII Уголовного кодекса Российской Федерации «Преступления в сфере экономики» и практики их применения показал существенное расхождение между юридически закрепленными и фактическими видами преступлений в сфере экономики, совершаемыми с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет.

Так, в указанном разделе Особенной части УК РФ содержится только две статьи, в которых упоминаются информационно-телекоммуникационные сети: ст. 159[6] «Мошенничество в сфере компьютерной информации» и ст. 171[2] «Незаконные организация и проведение азартных игр». Первая уголовно-правовая норма была введена федеральным законом от 29 ноября 2012 г. № 207-ФЗ[4], а вторая — федеральным законом от 20 июля 2011 г. № 250-ФЗ[5].

Приведем статистические сведения о количестве осужденных за данные преступления, предоставленные Судебным департаментом при Верховном Суде Российской Федерации (табл.)[6].

Количество осужденных по ст. 159[6] и 171[2] УК РФ в 2013 г. — первом полугодии 2016 г., чел.

Number of persons convicted according to Art. 159[6] and 171[2] of the Criminal Code of the Russian Federation in 2013 — the first half of 2016

Статья УК РФ / Article of the CC of the RF	Количество осужденных / Number of convicted persons			
	2013	2014	2015	2016 (6 месяцев) / 2016 (6 months)
Статья 159[6] / Article 159[6]	57	92	110	212
Статья 171[2] / Article 171[2]	57	113	496	31

Полагаем, что эти статистические данные следует оценивать критически, учитывая высокую латентность таких преступлений, обусловленную рядом факторов, в том числе практическими трудностями в их выявлении и доказывании. Именно такие проблемы отметили 119 (94,4 %) из 126 опрошенных нами сотрудников правоохранительных органов. Кроме того, опрос данных респондентов, а также 78 судей и 95 научно-педагогических работников показал, что к числу преступлений в сфере экономики, для которых использование информационно-телекоммуникационных сетей является типичным способом их совершения, можно отнести: 1) причинение имущественного ущерба путем обмана или злоупотребления доверием (ст. 165 УК РФ) — 70,6 % опрошенных сотрудников правоохранительных органов, 61,5 % судей, 88,4 % научно-педагогических работников; 2) незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ), — 54,0 % сотрудников правоохранительных органов, 52,6 % судей, 75,8 % научно-педагогических работников; 3) неправомерное использование инсайдерской информации (ст. 185[6] УК РФ) — 44,4, 39,7 и 66,3 % соответственно.

Информационно-телекоммуникационные сети могут использоваться и для совершения экономических преступлений, связанных с приобретением и сбытом определенных предметов,

[4] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации : федер. закон от 29 нояб. 2012 г. № 207-ФЗ // Собрание законодательства РФ. 2012. № 49. Ст. 6752.

[5] О внесении изменений в отдельные законодательные акты Российской Федерации : федер. закон от 20 июля 2011 г. № 250-ФЗ // Там же. 2011. № 30, ч. 1. Ст. 4598.

[6] Данные судебной статистики [Электронный ресурс] // Судебный департамент при Верховном Суде Российской Федерации : офиц. сайт. URL: http://www.cdep.ru/index.php?id =79.

в том числе поддельных денег, ценных бумаг, банковских карт, а также данных действующих банковских карт [3; 7]. Однако в таком случае использование сети Интернет или других информационно-телекоммуникационных сетей является одним из возможных способов совершения соответствующих преступлений и, как правило, не придает им какую-либо специфику, т.е. выступает в качестве их факультативного признака. Например, данные действующих банковских карт позволяют совершать покупки в интернет-магазинах без специального ПИН-кода. В Интернете к продаже активно предлагаются двухсторонние изображения банковских карт, а также их ПИН-коды, при наличии которых можно изготовить поддельные аналоги таких карт и оплачивать с их помощью товары в обычных магазинах. Также через ресурсы сети Интернет продаются и покупаются скиммеры (приборы, устанавливаемые на банкоматах, позволяющие считать данные банковской карты) [1]. Вне связи с конкретным преступлением многие из подобных действий (например, предоставление данных действующей банковской карты или продажа скиммера) не являются уголовно наказуемыми, что представляет собой пробел в праве.

Опрос респондентов и изучение уголовных дел показали, что информационно-телекоммуникационные сети хотя и не используются при выполнении объективной стороны других преступлений в сфере экономики, однако задействуются в процессе приготовления к ним, в том числе для поиска нужной информации, обмена сведениями, приобретения необходимых орудий и средств, подыскания соучастников преступления и сговора с ними на совместное совершение последнего. То есть использование информационно-телекоммуникационных сетей в настоящее время является одним из обязательных либо факультативных объективных признаков ряда составов преступлений в сфере экономики, кроме того, такие сети фактически выступают средством, которое может применяться в ходе приготовления к любым уголовно наказуемым деяниям экономической направленности.

В результате изучения материалов 120 уголовных дел (44 дела о мошенничестве в сфере компьютерной информации, 31 дело об организации азартных игр, 15 дел о причинении имущественного ущерба путем обмана или злоупотребления доверием, 11 дел о незаконных получении и разглашении сведений, составляющих коммерческую, налоговую или банковскую тайну, и 19 дел об иных преступлениях в сфере экономики) и опроса указанных выше респондентов мы пришли к выводу, что использование информационно-телекоммуникационных сетей для приготовления и (или) последующего совершения рассматриваемых преступлений, как правило, придает соответствующей криминальной деятельности усложненный, профессиональный характер, предполагающий применение виновными знаний, умений и навыков в области информационных технологий, превышающих уровень обычных компьютерных пользователей; позволяет планировать свое преступное поведение и дальнейшее сокрытие его следов, а также направления использования и легализации преступно полученного имущества, пользоваться возможностями и преимуществами удаленного совершения преступления; увеличивает масштаб и расширяет спектр причиняемых общественно опасных последствий. Помимо этого, 23 % опрошенных сотрудников правоохранительных органов отметили, что в ходе оперативно-розыскного сопровождения уголовных дел о таких преступлениях ими были выявлены сведения об организованном и транснациональном характере данной преступной деятельности. Эти обстоятельства также отмечаются в теоретических исследованиях [1; 6; 8].

Выделенные особенности анализируемых преступлений осложняют деятельность по их предупреждению и ставят перед необходимостью выработки комплекса научно обоснованных рекомендаций, направленных на повышение эффективности соответствующей превентивной деятельности, в том числе на придание ей системного характера. Предупреждение таких преступлений должно строиться с учетом общих принципов и устоявшегося содержания такой деятельности и одновременно учитывать особенности рассматриваемых уголовно наказуемых деяний и лиц, их совершающих, современное состояние законодательства и правоохранительной деятельности в данной области [6; 9].

В результате проведенного нами опроса респондентов было установлено, что первоочередным направлением в повышении эффективности предупреждения рассматриваемых преступлений является совершенствование законодательства, в том числе УК РФ. Данное направление выделили 88,9 % опрошенных сотрудников правоохранительных органов, 80,8 % судей и 94,7 % научно-педагогических работников.

Применительно к установлению уголовной ответственности за мошенничество в сфере компьютерной информации в первую очередь отметим, что мы поддерживаем позицию, высказанную Л.Д. Гаухманом, о том, что данный вид хищения законодатель необоснованно отнес к числу преступлений с привилегированным составом (в санкции ч. 1 ст. 159[6] УК РФ отсутствует наказание в виде лишения свободы, тогда как в санкции общей нормы, предусмотренной ч. 1 ст. 159 УК РФ, мошенничество наказывается вплоть до лишения свободы на срок до двух лет) [7]. Выше мы уже говорили, что преступления, совершаемые с использованием информационно-телекоммуникационных сетей, являются более сложными и по меньшей мере не уступают в своей общественной опасности аналогичным деяниям, при осуществлении которых данные сети не использовались. Поэтому считаем явным недочетом законодателя смягчение ответственности за мошенничество в сфере компьютерной информации. С этим мнением согласились 83,3 % опрошенных сотрудников правоохранительных органов, 70,5 % судей и 94,7 % научно-педагогических работников. Также судьи обратили внимание на очевидную неточность, содержащуюся в санкции ч. 1 ст. 159[6] УК РФ, состоящую в указании наказания в виде принудительных работ при отсутствии его альтернативности по отношению к лишению свободы, в санкции отсутствующего. Это противоречит ч. 1 ст. 53[1] УК РФ, согласно которой принудительные работы могут быть назначены только как альтернатива лишению свободы. Вследствие данной неточности санкция ч. 1 ст. 159[6] УК РФ еще более смягчилась, что снизило ее предупредительный эффект.

Кроме того, считаем, что применение ст. 159[6] УК РФ осложняет и тот факт, что деяние, ею запрещенное, названо мошенничеством, поскольку таковое всегда должно состоять в обмане или злоупотреблении доверием, тогда как виновные лица чаще всего не используют данные способы, поскольку воздействуют непосредственно на те или иные ресурсы информационно-телекоммуникационных сетей, минуя необходимость вводить кого-либо в заблуждение. Мы не согласны с мнением А.А. Комарова, предлагающего расширить понимание обмана, распространив его на воздействие не только на человека, но и на автоматизированные компьютерные системы [6]. Считаем, что обмануть или ввести в заблуждение можно только человека, а не компьютер. Поэтому более правильным нам видится включение квалифицирующего признака в виде использования информационно-телекоммуникационных сетей или иных информационных технологий для совершения хищения в уже существующие нормы гл. 21 УК РФ либо ее дополнение новой статьей об ответственности за хищение в сфере компьютерной информации. Опрос показал приоритетность первого варианта данного предложения — его поддержали 72,2 % респондентов из числа сотрудников правоохранительных органов, 58,9 % судей и 93,7 % научно-педагогических работников.

Относительно незаконных организации и проведения азартных игр в качестве положительного момента развития соответствующего уголовно-правового запрета отметим изменение конструкции состава преступления, предусмотренного ч. 1 ст. 171[2] УК РФ, с материальной на формальную, позволившее на практике привлекать к ответственности за сам факт совершения указанных незаконных действий [10]. Вместе с тем анализ результатов опроса показал целесообразность совершенствования данной нормы, в том числе в виде дифференциации уголовной ответственности лиц, незаконно организовавших и проводивших азартные игры, с установлением более строгого наказания за действия первых из них. Это предложение нашло одобрение у 52,4 % опрошенных сотрудников правоохранительных органов, 48,7 % судей и 77,9 % научно-педагогических работников.

Отметим, что, в отличие от незаконных получения и разглашения сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ), уголовные дела о неправомерном использовании инсайдерской информации (ст. 185[6] УК РФ) на практике отсутствуют. Это не в последнюю очередь связано со сложностью понятий, относящихся к инсайдерской информации, искусственной конкуренцией данных уголовно-правовых норм и материальной конструкцией состава преступления, предусмотренного ст. 185[6] УК РФ. Так, по данным Судебного департамента при Верховном Суде Российской Федерации, в 2014-м, 2015-м и в первом полугодии 2016 г. по ст. 185[6] УК РФ осужденных не было. Учитывая данные обстоятельства, предлагаем расширить понятие коммерческой, налоговой и банковской тайны с одновременным признанием ст. 185[6] УК РФ утратившей

силу. Данное предложение поддержали 58,7 % респондентов из числа сотрудников правоохранительных органов, 38,5 % судей и 86,3 % научно-педагогических работников.

Нами были изучены и уголовные дела о причинении имущественного ущерба путем обмана или злоупотребления доверием (ст. 165 УК РФ), которое также может совершаться с использованием информационно-телекоммуникационных сетей (в 11 из 15 проанализированных уголовных дел). Данное преступление наиболее сходно с мошенничеством и, по нашему мнению, обладает не меньшей общественной опасностью, однако законодатель в 2011 г. включил в число обязательных признаков состава рассматриваемого преступления крупный размер причиняемого ущерба, что оставило вне сферы уголовной ответственности подавляющее большинство деяний, ранее подпадавших под действие ст. 165 УК РФ. Данное законодательное изменение мы находим необоснованным, с чем согласились 70,6 % опрошенных сотрудников правоохранительных органов, 92,6 % судей и 77,9 % научно-педагогических работников. Также респонденты поддержали наше предложение о дополнении ст. 165 и 183 УК РФ квалифицирующим признаком в виде совершения преступления с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет (50,8, 43,6 и 81,1 % опрошенных соответственно).

Анализ материалов уголовных дел и опрос работников правоохранительных органов позволили нам сделать вывод о необходимости совершенствования и других нормативных правовых актов, направленных на предупреждение преступности [8].

Прежде всего, это Федеральный закон «Об основах системы профилактики правонарушений в Российской Федерации» от 23 июня 2016 г. № 182-ФЗ[7], в котором отсутствуют положения, учитывающие специфику предупреждения преступлений, совершаемых с использованием информационно-телекоммуникационных сетей.

Также считаем целесообразным внести изменения и дополнения в Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ[8] и постановление Правительства Российской Федерации от 26 октября 2012 г. № 1101 об утверждении правил создания, формирования единого реестра доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети Интернет, содержащих информацию, распространение которой в России запрещено[9]. В криминологии уже высказывалась позиция о необходимости совершенствования нормативного регулирования деятельности по выявлению ресурсов сети Интернет, содержащих запрещенную информацию, касающуюся совершения противоправных деяний, и обеспечению реализации данного запрета. В частности, предлагается возложить на Федеральную налоговую службу полномочия по включению сведений, касающихся незаконных организации и проведения азартных игр, в указанный реестр, разработать критерии оценки интернет-сайтов на предмет содержания запрещенной информации, ввести административную ответственность для интернет-провайдеров за обеспечение доступа к ресурсам, содержащим запрещенную информацию [9; 10]. Соглашаясь с данными предложениями, отметим необходимость формирования единой, согласованной системы правовых и иных средств, направленных на предупреждение рассматриваемых преступлений.

Полагаем, что сотрудничающие государства должны стремиться к укреплению и расширению взаимодействия в области противодействия преступности, в том числе преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей. Заключение двухсторонних и многосторонних договоров в этой области будет способствовать унификации правовых средств, направленных на предупреждение, выявление, раскрытие и доказывание таких преступлений [3; 8].

При опросе сотрудников правоохранительных органов в качестве других проблем предупреждения экономических преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, подлежащих решению, были названы: 1) недостаточ-

[7] Собрание законодательства РФ. 2016. № 26, ч. 1. Ст. 3851.

[8] Там же. 2006. № 31, ч. 1. Ст. 3448.

[9] О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено : постановление Правительства РФ от 26 окт. 2012 г. № 1101 // Собрание законодательства РФ. 2012. № 44. Ст. 6044.

ная техническая оснащенность подразделений (88,1 % респондентов); 2) потребность в расширении штатной численности и более четком распределении компетенции подразделений и их сотрудников (73,0 %); 3) недостатки в техническом обеспечении безопасности финансовых и иных экономических отношений, связанных с использованием информационно-телекоммуникационных сетей и других информационных технологий (68,3 %); 4) необходимость совершенствования образовательной подготовки и повышения квалификации таких сотрудников (62,7 %); 5) отсутствие налаженной разъяснительной деятельности по информированию организаций и населения о противоправности соответствующих действий, правовых последствиях их совершения и способах обеспечения информационной безопасности и защищенности их денежных средств и иного имущества от таких посягательств (54,0 %).

Отметим, что при изучении правоприменительной практики по выделенным преступлениям, особенно причинившим имущественный ущерб, наиболее часто выясняется наличие проблем, указанных в третьем и пятом пунктах. Например, они находят свое отражение почти во всех уголовных делах о мошенничествах в сфере компьютерной информации, совершенных в отношении граждан.

Так, К., имея доступ к ранее похищенному мобильному телефону потерпевшей П., получил на указанный телефон с подключенной к сим-карте услугой «Мобильный банк» смс-оповещение от ОАО «Сбербанк России» в виде информации о движении денежных средств по лицевому счету банковской карты, принадлежащей П., и о возможности управления счетом карты посредством смс-сообщений. Во исполнение возникшего умысла на хищение чужих денежных средств К., зная о возможностях управления лицевым счетом карты посредством услуги «Мобильный банк», сформировал смс-запрос о наличии денежных средств на лицевом счете банковской карты, принадлежащей П., и, получив смс-сообщение банка о доступном лимите денежных средств, сформировал смс-запросы на специальный номер 900 о переводе денежных средств с указанной банковской карты потерпевшей на лицевой счет принадлежащего ему мобильного телефона, тем самым выполнив финансовые транзакции по списанию денежных средств в размере 7 500 и 8 000 р., которые в последующем перевел с лицевого счета своего мобильного телефона на лицевой счет своей банковской карты[10].

Приведенный пример демонстрирует нам, что в настоящее время отсутствует необходимая степень защищенности денежных средств, находящихся на банковской карте, от указанных противоправных действий. Вместе с тем потерпевшая, зная о хищении своего телефона и подключенной к номеру услуге «Мобильный банк», в течение длительного времени (более суток) не предпринимала действий по блокированию средств на своем лицевом счете, не отключала услугу «Мобильный банк» и не блокировала сим-карту своего телефона. Подчеркнем, что данный пример являет собой один из типичных вариантов хищения денежных средств с банковских карт граждан, которые, по сути, нередко сами создают предпосылки для совершения таких преступлений.

Помимо информирования граждан, особенно работников банковских, прочих кредитных и иных организаций, о новых способах совершения преступлений, в том числе с использованием информационных технологий, необходимо развивать специальные курсы для обучения и повышения квалификации сотрудников правоохранительных органов в области предупреждения соответствующих преступлений [2; 4].

Опрос практических сотрудников правоохранительных органов и анализ теоретических источников, посвященных данной проблематике, позволил нам предложить следующие специальные меры предупреждения рассматриваемых преступлений: 1) повсеместное введение и обеспечение обязательной и достаточной идентификации личности пользователя при предоставлении доступа в сеть Интернет в местах коллективного пользования; 2) создание условий для разработки и реализации государственной программы, связанной с внедрением электронной подписи в гражданский оборот, присвоением каждому пользователю сети Интернет электронного сертификата, в содержание которого входят персональные данные о его владельце, позволяющие произвести его идентификацию; 3) принятие правовых и организационных мер для исключения возможности создания и использования анонимных электронных почтовых ящиков без заключения письменного договора с провайдером; 4) усложнение системы иден-

[10] Апелляционное постановление Иркутского областного суда от 5 мая 2015 г. // Архив Иркутского областного суда за 2015 г.

ISSN 2500-4255

тификации пользователя, производящего финансовые транзакции со своих лицевых счетов с использованием мобильных и онлайн-приложений [1; 6; 9; 10].

В заключение отметим, что предупреждение рассматриваемых уголовно наказуемых деяний должно быть встроено в общую систему предупреждения преступлений, совершаемых с использованием информационно-телекоммуникационных сетей. Элементы современной преступности тесно переплетены и взаимосвязаны, поэтому превентивные меры также должны иметь согласованный, дополняющий друг друга характер и в своей совокупности представлять единую систему противодействия преступности, ориентированную на эффективную защиту личности, общества и государства от общественно опасных посягательств.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение / Д.Н. Карпова // Власть. — 2014. — № 8. — С. 46–50.

2. Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime / R. Broadhurst, P. Grabosky, M. Alazab, S. Chon // International Journal of Cyber Criminology. — 2014. — Vol. 8, iss. 1. — P. 1–20.

3. Holt T.J. Exploring Stolen Data Markets Online: Products And Market Forces / T.J. Holt, E. Lampke // Criminal Justice Studies. — 2010. — Vol. 23 (1). — P. 33–50.

4. Spapens T. Macro Networks, Collectives, and Business Processes: An Integrated Approach to Organized Crime / T. Spapens // European Journal of Crime, Criminal Law and Criminal Justice. — 2010. — Vol. 18, iss. 2. — P. 185–215.

5. Борисов С.В. Преступления экстремистской направленности: проблемы законодательства, теории и практики : дис. … д-ра юрид. наук : 12.00.08 / С.В. Борисов. — М., 2012. — 484 с.

6. Комаров А.А. Криминологические аспекты мошенничества в глобальной сети Интернет : дис. … канд. юрид. наук : 12.00.08 / А.А. Комаров. — Пятигорск, 2010. — 262 с.

7. Гаухман Л.Д. Мошенничество: новеллы уголовного законодательства / Л.Д. Гаухман // Уголовное право. — 2013. — № 3. — С. 25–27.

8. Лагуточкин А.В. О проблеме правового регулирования использования сети Интернет в условиях обеспечения безопасности государства / А.В. Лагуточкин // Проблемы правоохранительной деятельности. — 2012. — № 1. — С. 33–37.

9. Горовенко С.В. Проблема предупреждений правонарушений в сфере игорного бизнеса в сети Интернет / С.В. Горовенко, Е.С. Изюмова // Вестник Челябинского государственного университета. Сер.: Право. — 2015. — № 17, вып. 43. — С. 25–29.

10. Гаджиева А.А. Меры предупреждения незаконной организации азартных игр и проблемы их совершенствования / А.А. Гаджиева, А.М. Дамадаева // Евразийский юридический журнал. — 2015. — № 11. — С. 199–202.

REFERENCES

1. Karpova D.N. Cybercrimes: a global issue and its solution. *Vlast' = The Power*, 2014, no. 8, pp. 46–50. (In Russian).

2. Broadhurst R., Grabosky P., Alazab M., Chon S. Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology*, 2014, vol. 8, iss. 1, pp. 1–20.

3. Holt T.J., Lampke E. Exploring stolen data markets online: products and market forces. *Criminal Justice Studies*, 2010, vol. 23 (1), pp. 33–50.

4. Spapens T. Macro networks, collectives, and business processes: an integrated approach to organized crime. *European Journal of Crime, Criminal Law and Criminal Justice,* 2010, vol. 18, iss. 2, pp. 185–215.

5. Borisov S.V. *Prestupleniya ekstremistskoi napravlennosti: problemy zakonodatel'stva, teorii i praktiki. Dokt. Diss.* [Extremism crimes: issues of legislation, theory and practice. Doct. Diss.]. Moscow, 2012. 484 p.

6. Komarov A.A. *Kriminologicheskie aspekty moshennichestva v global'noi seti Internet. Kand. Diss.* [Criminological aspects of fraud in the Internet global network. Cand. Diss.]. Pyatigorsk, 2010. 262 p.

7. Gaukhman L.D. Fraud: stories of criminal law. *Ugolovnoe pravo = Criminal Law*, 2013, no. 3, pp. 25–27. (In Russian).

8. Lagutochkin A.V. On the problem of the legal regulation of Internet network use in conditions of the provision of state safety. *Problemy pravookhranitel'noi deyatel'nosti = Problems of law Enforcement*, 2012, no. 1, pp. 33–37. (In Russian).

9. Gorovenko S.V., Izyumova E.S. Problem of the prevention of offenses in the online-gaming sphere. *Vestnik Chelyabinskogo gosudarstvennogo universiteta. Seriya: Pravo = Bulletin of Chelyabinsk State University. Series: Law*, 2015, no. 17, iss. 43, pp. 25–29. (In Russian).

10. Gadzhieva A.A., Damadaeva A.M. Preventive measures of the illicit gambling and problems of its improvement. *Evraziiskii yuridicheskii zhurnal = Eurasian Law Journal*, 2015, no. 11, pp. 199–201. (In Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Суходолов Александр Петрович — ректор Байкальского государственного университета, доктор экономических наук, профессор, заслуженный экономист Российской Федерации, г. Иркутск, Российская Федерация; e-mail: rector@bgu.ru.

Иванцов Сергей Вячеславович — профессор кафедры криминологии Московского университета МВД России им. В.Я. Кикотя, доктор юридических наук, профессор, г. Москва, Российская Федерация; e-mail: isv1970@mail.ru.

INFORMATION ABOUT THE AUTHORS

Sukhodolov, Alexander P. — Rector, Baikal State University, Doctor of Economics, Professor, Honored Economist of the Russian Federation, Irkutsk, the Russian Federation; e-mail: rector@bgu.ru.

Ivantsov, Sergey V. — Professor, Chair of Criminology, V.Ya. Kikotya Moscow University of the Ministry of Internal Affairs of Russia, Doctor of Law, Professor, Moscow, the Russian Federation; e-mail: isv1970@mail.ru.

Борисов Сергей Викторович — ведущий научный сотрудник Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, доктор юридических наук, доцент, г. Москва, Российская Федерация; e-mail: svb8@yandex.ru.

Спасенников Борис Аристархович — главный научный сотрудник Научно-исследовательского института Федеральной службы исполнения наказаний России, доктор юридических наук, доктор медицинских наук, профессор, г. Москва, Российская Федерация; e-mail: borisspasennikov@yandex.ru.

БИБЛИОГРАФИЧЕСКОЕ ОПИСАНИЕ СТАТЬИ

Суходолов А.П. Актуальные проблемы предупреждения преступлений в сфере экономики, совершаемых с использованием информационно-телекоммуникационных сетей / А.П. Суходолов, С.В. Иванцов, С.В. Борисов, Б.А. Спасенников // Всероссийский криминологический журнал. — 2017. — Т. 11, № 1. — С. 13–21. — DOI: 10.17150/2500-4255.2017.11(1).13-21.

Borisov, Sergey V. — Leading Researcher, Institute of Legislation and Comparative Law of the Government of the Russian Federation, Doctor of Law, Ass. Professor, Moscow, the Russian Federation; e-mail: svb8@yandex.ru.

Spasennikov, Boris A. — Chief Researcher, Research Institute of Federal Penitentiary Service of Russia, Doctor of Law, Doctor of Medicine, Professor, Moscow, the Russian Federation; e-mail: borisspasennikov@yandex.ru.

BIBLIOGRAPHIC DESCRIPTION

Sukhodolov A.P., Ivantsov S.V., Borisov S.V., Spasennikov B.A. Topical issues of preventing economic crimes committed with the use of information and telecommunication networks. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2017, vol. 11, no. 1, pp. 13–21. DOI: 10.17150/2500-4255.2017.11(1).13-21. (In Russian).