

Социально-правовое обоснование введения уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

Новичков Валерий Евгеньевич,

доктор юридических наук, доцент, профессор кафедры уголовного права юридического факультета Юго-Западного государственного университета
Курск, Россия. valery.novichkov@yandex.ru

Пыхтин Иван Геннадьевич,

аспирант кафедры уголовного права юридического факультета Юго-Западного государственного университета
Курск, Россия. e-mail: abcqir@gmail.com

Интегрирование отечественных информационных, информационно-коммуникационных и иных кибернетических сетей и систем в мировую информационную архитектуру, оснащение компьютерного оборудования импортными комплектующими, а также применение иностранного программного обеспечения в сочетании с постоянными неправомерными воздействиями на информационную инфраструктуру российского общества, равно как на критическую информационную инфраструктуру государства, порождают новые угрозы информационной и общей безопасности Российской Федерации. Повреждение информационной составляющей критической информационной инфраструктуры с большой долей вероятности может привести к катастрофическим социально-экономическим потерям в силу ее значимости как связующего звена между другими секторами государственной и общественной инфраструктуры, что неизбежно нанесет вред и этим секторальным объектам. Опасность для критической информационной инфраструктуры Российской Федерации представляют и воздействия на нее, совершаемые в незаконных, преступных, террористических, военных, рейдерских, дискредитационных и иных целях со стороны некоторых лиц, социально-психологических групп, образований и иностранных государств в лице их специальных служб. Динамика преступлений в сфере компьютерной информации в России, а также анализ уголовного законодательства, внесенных в него изменений и дополнений за 20 лет показали необходимость и своевременность имплементации уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации и усиления противодействия данному виду общественно опасного деяния.

Ключевые слова: преступления в сфере компьютерной информации; компьютерный вирус; компьютерная атака; информационная архитектура; стратегически важные информационные объекты; критическая информационная инфраструктура.

Для цитирования: Новичков В. Е., Пыхтин И. Г. Социально-правовое обоснование введения уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // Психопедагогика в правоохранительных органах. 2018. № 2(73). С. 25–29.

Возможности злоупотреблений при эксплуатации современной компьютерной техники, аппаратно-технических средств и информационных технологий настолько широки, насколько безграничен потенциал использования компьютерных систем и их сетей. Так, на самых ранних этапах повсеместного внедрения кибернетических устройств общественно опасные деяния, совершаемые с их помощью, мало чем отличались от общеуголовных преступлений. Как правило, это были хищения денежно-валютных средств путем компьютерного перевода денег со счетов различных депонентов на собственные счета и обратно (получение процентной прибыли); мошенничество посредством предоставления заведомо ложной, частичной или любой иной сходной информации в программу или отчетность, которая влечет выгоду для лица, совершившего преступление, и убытки для любого другого лица; саботаж в виде полного или частичного использования новых технологий с различными корыстными целями и др. В реестрах учета компьютерных преступлений Российской Федерации содержится немало

сведений о ранних общественно опасных деяниях, совершенных с помощью ЭВМ (например, несанкционированный перевод денег со счетов клиентов американского City Bank of America на общую сумму более 10 млн долларов на счета преступной группы во главе с программистом Левиным Владимиром в 1994 г. и др.) [1, с. 17; 2, с. 42–47].

С течением времени число компьютерных преступлений и круг общественных отношений, на которые они посягали постоянно, увеличивались, как и география их совершения, а сами такие общественно опасные деяния приобретали иные количественно-качественные характеристики, видоизменяясь и трансформируясь в преступления в сфере компьютерной информации, которые сейчас не знают государственно-территориальных границ.

Для защиты компьютерных коммуникаций и компьютерной информации, образов устройств управления компьютерами и баз данных 23 сентября 1992 г. в Российской Федерации был принят Закон № 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных»¹, который причислил защиту

¹ О правовой охране программ для электронных вычислительных машин и баз данных : закон Российской Федерации от 23 сентября 1992 г. № 3523-1 (ред. от 02.02.2006) // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1992. № 42, ст. 2325.

программ для ЭВМ к защите произведений литературы, а их базам данных предоставил правовую охрану как творческим сборникам, тем самым отнес их к объектам авторского права. Кроме того, ст. 20 этого Закона предусматривала уголовную ответственность за выпуск под своим именем чужой программы для ЭВМ или базы данных либо незаконное воспроизведение или распространение таких произведений. Однако масштабные перемены в экономической и политической жизни Российской Федерации во второй половине 1980–1990-х гг. и проводимые судебно-правовые преобразования, включая уголовно-правовую реформу, не позволили внести упомянутую новеллу в уголовное законодательство того времени (УК РСФСР 1960 г.).

Вместе с тем необходимо отметить, что действующие в указанный период нормативные акты уголовно-правового и иного характера, регулирующие использование кибернетического информационного пространства России, отличались не только устаревшими и несовершенными положениями, но и их изъятиями, а также вносимыми в текущее законодательство изменениями, дополнениями и новеллами, касающимися искусственного гиппокампа. Кроме того, в стране активно обсуждались проекты и концепции нового Уголовного кодекса Российской Федерации, которые предусматривали до 6 видов «компьютерных преступлений»². Тем не менее в окончательном варианте Уголовного кодекса РФ 1996 г. было закреплено всего три состава преступлений в сфере компьютерной информации и помещенных в отдельную главу: «За неправомерный доступ к компьютерной информации» (ст. 272), «Создание, использование и распространение вредоносных программ для ЭВМ» (ст. 273), «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» (ст. 274).

Иные общественно опасные деяния, включая посяательства на критически важные конструкты государственной инфраструктуры, объекты критической информационной инфраструктуры, с использованием компьютерной техники, ее программного обеспечения, компьютерных технологий, электронно-коммуникационных приборов, гаджетов, андроидов и т. п. к разряду преступлений против компьютерной информации в новом УК РФ 1996 г. отнесены не были. Согласно УК РФ ответственность за подобные неправомерные действия должна была наступать по иным статьям его Особенной части, в соответствии с их родовым и непосредственным объектами. Компьютерная информация в подобных случаях выступала как орудие или средство совершения преступления, а такие деяния могли квалифицироваться по правилам совокупности — с преступлениями, предусмотренными ст. ст. 272–274 УК РФ.

Конкретизация общего, родового и непосредственного объектов и предметов неправомерного воздействия на сферу компьютерной информации в УК РФ немедленно отразилась на текущей реализации уголовной ответственности. Число зарегистрированных преступлений за неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ, нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. ст. 272–274 УК РФ) за пять последующих лет выросло в 275 раз, а за девять лет (с 1997 г. по 2005 г.) почти в 310 раз.

На указанном отрезке времени 50% всех видов компьютерных преступлений относятся к незаконному доступу к компьютерной информации при этом данный вид общественно опасных деяний свидетельствует о росте преступности корыстной, групповой, молодежной и трансграничной направленности. Специалисты подчеркивают, что преступления в сфере компьютерной информации, как правило, становятся лишь первым звеном в цепи многих общественно опасных правонарушений, от общеуголовных (кражи, вымогательства, мошенничества) до особо тяжких (кибертерроризм, киберэкстремизм, посягательства на сети электросвязи и другие особо важные объекты инфраструктуры) [3]. Тем не менее статистические данные, оценки экспертов говорят о том, что период активного роста количества этих преступлений в России закончился в 2006 г. (например, в 2004 г. было зарегистрировано 13 261 подобное преступление, в 2005 г. — 14 810, в 2006 г. — чуть более 14 000 преступлений) (табл.).

Явная направленность распространения и значительный рост киберпреступных деяний, ориентированных в большей степени на сферу компьютерной информации, не могли не повлиять на очередное принятие поправок в УК РФ. Федеральный закон от 7 декабря 2011 г. № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» подверг значительным изменениям и дополнениям многие уголовно-правовые нормы, в том числе относящиеся к преступлениям в сфере компьютерной информации (ст. ст. 272, 273, 274 УК РФ). Согласно первой редакции ст. 272 УК РФ «Неправомерный доступ к охраняемой законом компьютерной информации» ответственность должна была наступать за доступ к любой информации на машинном носителе, в электронно-вычислительной машине, системе ЭВМ или их сети, если он влечет уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети (ч. 1), а квалифицированным при-

² О внесении изменений и дополнений в Уголовный кодекс РСФСР : закон РФ от 18 февраля 1993 г. № 4512-1 // Там же. 1993. № 10, ст. 362 ; О правовой охране топологий интегральных микросхем : закон РФ от 23 сентября 1992 г. № 3526-1 // Там же. 1992. № 42, ст. 2328 ; О внесении изменений и дополнений в Уголовный кодекс РСФСР и Уголовно-процессуальный кодекс РСФСР : федеральный закон от 1 июля 1994 г. № 10-ФЗ (ред. от 18.12.2001) // Собрание законодательства Российской Федерации. 1994. № 10, ст. 1109 ; Об информации, информатизации и защите информации : федеральный закон от 20 февраля 1995 г. № 24-ФЗ // Там же. 1995. № 8, ст. 609 ; Уголовный кодекс Российской Федерации : проект // Там же. 1992. № 42, ст. 2326.

знаком считалось «то же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети» (ч. 2). В редакции Федерального закона от 7 декабря 2011 г. № 420-ФЗ под «неправомерный доступ к компьютерной информации» подпадало «деяние, которое повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации» (ч. 1 ст. 272 УК РФ), а квалифицированные виды данного состава включали деяния: а) причинившие крупный ущерб или совершенные из корыстной заинтересованности (ч. 2); б) предусмотренные чч. 1 и 2, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения (ч. 3); в) указанные в чч. 1–3, если они повлекли тяжкие последствия или создали угрозу их наступления (ч. 4). Кроме того, ст. 272 УК РФ содержала два примечания с определением понятий: 1) компьютерная информация — сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи; 2) крупный ущерб, относящийся ко всем статьям главы 28 УК РФ, — ущерб, сумма которого превышает один миллион рублей.

Перечисленные нововведения в УК РФ не повлияли на дальнейшую динамику преступлений в сфере компьютерной информации, которая продолжила «синусоидальную регистрационную» тенденцию. Научные прогнозные оценки и судебно-следственная практика, регистрация общественно опасных деяний, их фиксация и возбуждение уголовных дел по «новым составам» преступлений, предусмотренных ст. ст. 272–274 УК РФ, в первые годы осуществлялись с определенной осторожностью, затем с нарастающей интенсивностью, и наконец регистрация и реагирование на преступления в сфере компьютерной информации стали стабильными, а к настоящему времени их «регистрационная» динамика, квалификация и практика применения приобрели устойчивый характер. Данное утверждение подкрепляется статистическими наблюдениями и научными исследованиями динамики, удельного веса и иных показателей зарегистрированных преступлений в сфере компьютерной информации за прошедшие 20 лет со дня вступления в законную силу главы 28 УК РФ [4, с. 68–70; 5, с. 9–10; 6, с. 110–157].

С 2012 г. развитие средств коммуникации, компьютерных систем, информационных ресурсов, всей сферы компьютерной информации в России вызвало определенные качественные, включая негативные, сдвиги в их использовании. Причем применение кибергиппокампа нередко проявлялось в неправомерном и агрессивном воздействии на стратегически важные информационные объекты инфраструктуры Российской Федерации. В то же время оперативное противодействие посягательствам на критическую информационную инфраструктуру страны усложняло

существующие правила эксплуатации виртуального пространства, которые позволяют обеспечить анонимность действий преступникам³. Например, в последнее время хакерским атакам и вирусным заражениям подвергались компьютерные системы таких российских компаний, как «Газпром» (вирус-шифровальщик Petya), «Роснефть», «Башнефть», «Хоум Кредит Банк», «МегаФон», «Вымпел-Ком», МВД России, Минздрав России, Минкомсвязь России и отдельные сегменты правительственной и спецсвязи (вирусная программа-шифровальщик WannaCry). Кроме того, организаторы этих кибератак нанесли удары по больницам, железнодорожному транспорту и полиции (причем подобные атаки могут быть организованы из любой точки мира, где есть доступ в интернет)⁴.

Исследования динамики преступлений против компьютерной информации рассматриваемого периода показывают значительные «годовые» расхождения их регистрационных показателей. Так, в 2012 г. всего было зарегистрировано 2820 преступлений (+4,5%) в сфере компьютерной информации, из них: неправомерный доступ к компьютерной информации (ст. 272 УК РФ) — 1930 фактов; создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) — 889; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) — 1 факт; в 2013 г. зафиксировано 2563 преступления (–9,1%); по ст. 272 УК РФ — 1799; ст. 273 — 764, а по ст. 274 УК РФ не было зарегистрировано ни одного преступления; в 2014 г. общее количество таких преступлений составило 1739 (без учета Крымского федерального округа — 1736)(–32,3%); по ст. 272 УК РФ — 1151; по ст. 273 — 585; по ст. 274 — 3 преступления; в 2015 г. зарегистрировано 2382 преступления (без учета Крымского федерального округа — 2377) (+36,9%); по ст. 272 УК РФ — 1396; по ст. 273 — 974; по ст. 274 — 12; в 2016 г. совершено 1748 преступлений (–26,6%); по ст. 272 УК РФ — 994; по ст. 273 — 751, по ст. 274 УК РФ — 3. Спойлер 2017 г. показал, что общее количество преступлений в сфере компьютерной информации составило 1863 (+7,6%).

Ученые с особым беспокойством отмечают, что с 2012 г. по настоящее время количественно-качественные характеристики совершаемых преступлений в сфере компьютерной информации позволяют заключить, что данные общественно опасные деяния представляют угрозу не только внутренней общественной безопасности страны, но и государственной безопасности, а также национальным интересам России [7, с. 219–224; 8, с. 1316–1325; 9, с. 101–110; 10, с. 90–95; 11, с. 105–111].

В связи с участвовавшими реальными киберугрозами 26 июля 2017 г. был принят, одобрен и подписан Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», вступивший в силу с 1 января 2018 г.⁵ Этот закон

³ Путин увидел наличие проблем в интернете из-за анонимности // Известия. 2018. 30 янв.

⁴ Кибератака на компьютеры МВД РФ обошлась без утечек информации // Рос. газета. 2017. 13 мая; Россия стала жертвой кибератаки // ТАСС — Новости в России и мире. 2017. 15 мая. URL: www.tass.ru (дата обращения: 14.11.2017).

гарантирует безопасность особо важным объектам информационной инфраструктуры Российской Федерации в целях бесперебойной деятельности ее категоризированных объектов из соответствующего реестра, в отношении которых возможны компьютерные атаки. Одновременно Федеральным законом от 31 июля 2017 г. № 194-ФЗ⁶ Уголовный кодекс Российской Федерации был дополнен ст. 274¹ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации». Данная уголовно-правовая норма предусматривает ответственность за создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации (ч. 1), и включает в себя четыре квалифицированных состава, к которым относятся: неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации (ч. 2); нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации (ч. 3); деяния, указанные выше (чч. 1, 2 или 3 ст. 274¹ УК РФ), совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения (ч. 4); все выше перечисленные деяния, если они повлекли тяжкие последствия.

Статья 274¹ УК РФ, призванная оградить критическую информационную инфраструктуру Российской Федерации от неправомерного преступного воздействия, объединила в себе не только основные объективно-субъективные признаки трех составов преступлений, предусмотренных ст. 272–274 УК РФ, но и интегрировала все сложности,

свойственные этим правовым предписаниям и порядку их юридической квалификации при установлении признаков основного и квалифицированных составов новой уголовно-правовой конструкции. Данное обстоятельство во многом компенсируется параметрами предмета преступления как критической информационной инфраструктуры Российской Федерации. Однако эти и другие проблемы, связанные с уголовной ответственностью за преступления, посягающие на критическую информационную инфраструктуру, а в целом на сферу компьютерной информации, выходят за рамки данной статьи.

Список литературы

1. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М., 2001. 496 с.
2. Стригалева Б. Р. Вопросы методики и тактики расследования уголовных дел о преступлениях, связанных с использованием компьютерной техники (на примере уголовного дела о хищении денежных средств Сити-банка) // Криминалистический семинар / отв. ред. В. В. Новик. СПб., 1998. Вып. 2. С. 42–43.
3. Кудрявцев В. Л. Преступления в сфере компьютерной информации: общая характеристика // Уголовное законодательство в XXI веке: современное состояние, проблемы трактовки и применения его положений с учетом задач дальнейшего укрепления экономического правопорядка : мат-лы междунар. науч.-практ. конф. (Нижний Новгород, 1 марта 2012 г.) / под ред. А. В. Козлова, П. Н. Панченко. Н. Новгород, 2012. С. 69–76.
4. Аванесов Г. А. Криминологическое прогнозирование и планирование борьбы с преступностью : учеб. пособие. М., 1972. 60 с.
5. Клейменов М. П. Уголовно-правовое прогнозирование. Томск, 1991. 169 с.
6. Новичков В. Е. Прогнозирование в сфере борьбы с преступностью в современной России : учеб. пособие. Курск, 2016. 300 с.
7. Чирков Д. К., Саркисян А. Ж. Преступность в сфере телекоммуникаций и компьютерной информации как угроза национальной безопасности страны // Актуальные проблемы экономики и права. 2013. № 3. С. 219–224.
8. Энгельгардт А. А. Уголовно-правовая оценка создания, использования и распространения вредоносных компьютерных программ (информации) // Lex Russica. 2014. № 11, Т. XCVI. С. 1316–1325.
9. Липинский Д. А., Евдокимов К. Н. Политические причины как современные факторы эволюции компьютерной преступности в Российской Федерации // Всероссийский криминологический журнал. 2015. Т. 9, № 1. С. 101–110.
10. Потапов С. А. Совершенствование расследования и раскрытия преступлений в сфере компьютерной информации // Социально-экономические явления и процессы. 2016. Т. 11, № 10. С. 90–95.
11. Ханов Т. А., Нуркеев А. Ж. Современные подходы к определению компьютерной преступности и особенности компьютерных преступлений // Известия Алтайского государственного университета. 2017. № 6(98). С. 105–111.

Поступила 25.12.2017

⁵ Собрание законодательства Российской Федерации. 2017. № 31, ч. 1, ст. 4736.

⁶ О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» : федеральный закон от 26 июля 2017 г. № 194-ФЗ// Там же. Ст. 4743.

Social and Legal Grounds providing Criminal Liability for Illegal Influence on Vital Informational Infrastructure of the Russian Federation

Novichkov Valery E.,

Doctor of Law, associate-professor, Professor at the department of Criminal Law, Law Faculty, Southwest State University
Kursk, Russia. e-mail: valery.novichkov@yandex.ru

Pykhtin Ivan G.,

post-graduate student of the department of Criminal Law, Law Faculty, Southwest State University
Kursk, Russia. e-mail: abcqip@gmail.com

Integration of national informational, information-communication and other cyber-nets and systems into the world informational architecture, equipping computer hardware with imported elements and use of foreign software together with persistent illegal influence on the informational infrastructure of the Russian society as well as on the vital national informational infrastructure are causing new threats to informational and entire security of the Russian Federation. Disruption of the informational element of the vital informational infrastructure is likely to cause catastrophic socially-economical damages due to its significance as a link between other sectors of the national and social infrastructure, which will inevitably be harmful for these sectors' objects. Threats for vital informational infrastructure of the Russian Federation are also revealed in situations of illegal, criminal, terrorist, military, raider, discrediting and other sorts of actions of some persons, social and psychological groups, entities and foreign countries presented by their intelligence services. Dynamics of cybercrimes in Russia and analysis of the criminal legislation, amendments made during twenty years proved it necessary and relevant to implant criminal liability for unlawful influence on the vital informational infrastructure of the Russian Federation and strengthen counteraction against this type of socially dangerous act.

Keywords: cybercrimes; computer virus; computer attack; informational architecture;
strategically important informational objects; vital informational infrastructure.

Citation: Novichkov V. E., Pykhtin I. G. Social and Legal Grounds providing Criminal Liability for Illegal Influence on Vital Informational Infrastructure of the Russian Federation. *Psychopedagogy in Law Enforcement*. No. 2(73). 2018. P. 25–29.

References

1. Volevodz A. G. Counteracting Cybercrimes: Legal Fundamentals of International Cooperation. Moscow, 2001. 496 p. (In Russ.)
2. Strigalev B. R. Questions of Methods and tactics of Computer Crimes Investigation (e.g. criminal case of embezzlement of money from Citybank. Criminalistics Seminar. Issue 2. Ed. by Novik V. V. St Petersburg, 1998. Pp. 42–43. (In Russ.)
3. Kudryavtsev V. L. Computer Information Crimes: General Characteristics. Criminal Law in the 21st century: Current State, Problems of Interpretation and Application with regard to the Tasks of Further Consolidation of Economic Law enforcement. Materials of International Conference (Nizhny Novgorod, March 1, 2012). Ed. by Kozlov A.V., Panchenko P.N. Nizhny Novgorod, 2012. Pp. 69–76. (In Russ.)
4. Avanesov G. A. Criminological Prognostication and Planning of Fighting Crime. Moscow, 1972. 60 p. (In Russ.)
5. Kleymenov M. P. Criminal Law Prognostication. Tomsk, 1991. 169 p. (In Russ.)
6. Novichkov V. E. Prognostication in Fighting Crime in Russia. Kursk, 2016. 300 p. (In Russ.)
7. Chirkov D. K., Sarkisyan A. Zh. Crime in Telecommunication and Computer Information as a Threat to National Security. *Actual Problems of Economics and Law*. No. 3. 2013. Pp. 219–224. (In Russ.)
8. Engelhardt A. A. Criminal Law Assessment of Creating, Using and Spreading Harmful Computer programmes (information). *Lex Russica*. No. 11. (vol. XCVI). 2014. Pp. 1316–1325. (In Russ.)
9. Lipinsky D. A., Evdokimov K. N. Political Reasons as Modern Factors of Computer Crime Evolution in the Russian Federation. *All-Russian Criminology Journal*. Vol.9 No. 1. 2015. Pp. 101–110. (In Russ.)
10. Potapov S. A. Enhancement of Investigation and Solution of Computer-related Crimes. *Social-Economic Phenomena and Processes*. Vol. 11. No. 10. 2016. Pp. 90–95. (In Russ.)
11. Khanov T. A., Nurkeev A. Zh. Modern Approaches to Definition of Computer Crimes and their Specifics. *Izvestiya of Altai State University Journal*. No. 6(98). 2017. Pp. 105–111. (In Russ.)