Аспекты обеспечения информационной безопасности Российской Федерации

Халиуллин А. И.,
научный сотрудник Научно-исследовательского института
Академии Генеральной прокуратуры РФ
E-mail: adel@lenta.ru

Аннотация. *В научной статье рассмотрены вопросы обеспечения международной информационной безопасности, составным элементом которой выступает информационная безопасности Российской Федерации. Высокотехнологичные способы и характеристика криминального пространства совершения преступлений в сфере компьютерной информации определяют их результативность. Вместе с тем отсутствует единая позиция государств в вопросах осуществления противодействия киберпреступности, что предопределено, в том числе, и разным уровнем проникновения информационных технологий. Усилия Российской Федерации в формировании правил сетевого взаимодействия, в том числе недопустимости нарушения информационного (сетевого) суверенитета государств, и иные предложения, выносимые на повестку рабочих групп в ООН, не находят поддержки у отдельных групп стран. Отсутствие общепризнанных границ в сетевом пространстве, а также процедур взаимодействия правоохранительных органов в целях противодействия киберпреступности формируют потенциально конфликтную информационную среду с относительно низким уровнем безопасности. Выявление, пресечение и расследование киберпреступлений в большинстве случаев осложнено трансграничным характером совершаемых деяний, что предполагает координацию усилий правоохранительных органов различных государств.*

В настоящее время в России реализуется комплекс мер, направленных на нормативное регулирование использования процессуальных документов в электронной форме в целях ускорения взаимодействия участников уголовного судопроизводства и сокращения сроков уголовного судопроизводства: вещественными доказательствами по уголовным делам служат электронные носители информации, содержащие электронные документы; введены отдельные элементы электронного документооборота. Однако законодательство Российской Федерации в информационной сфере, а также практика его применения нуждаются в дальнейшем совершенствовании.

Особое место среди субъектов противодействия распространению в сети Интернет информации, оборот которой ограничен на территории Российской Федерации, отводится органам прокуратуры РФ, которые не только осуществляют надзор за исполнением законов на всей территории России, но и непосредственно проводят работу по устранению причин и условий, способствовавших совершению киберпреступлений.

Ключевые слова*: информационная безопасность, киберпреступность, информатизация, прокурорский надзор, уголовное судопроизводство, юрисдикция.*

Всестороннее проникновение во все сферы жизнедеятельности человеческого общества информационных технологий обусловливает необходимость повышенного внимания всех государств к содержательному анализу вопросов обеспечения информационной безопасности.

Российская Федерация находится в цивилизационном русле развития мировых держав и испытывает, как и иные страны, возрастающие риски стремительной информатизации, особенно проявляющиеся в действиях, связанных с нанесением огромного невосполнимого вреда в различных областях деятельности общества и государства и относящихся в силу повышенной общественной опасности к числу преступных. В этой связи представляется недопустимой стигматизация отдельных государств, в том числе Российской Федерации, в качестве источников киберугроз в условиях отсутствия достоверной аргументации высказанных позиций[1].

В свою очередь рост объёмов информации, компьютерных сетей и числа пользователей, упрощение их доступа к сетевой информации существенно повышают опасность этих преступлений, в том числе в связи с совершением их посредством информационных технологий.

[1] Выступление заместителя Секретаря Совета Безопасности РФ О.В. Храмова на Саммите по вопросам кибербезопасности, Тель-Авив, 28.06.2017 // http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804268 (дата обращения: 20.07.2017).

Так, по оценкам специалистов, уровень агрессивности сетевой среды в первом квартале 2017 г. ярко характеризует то, что 26,67% пользователей персональных компьютеров с предустановленной антивирусной программой подверглись риску заражения вредоносными программами через сеть Интернет, а в абсолютных цифрах это несколько миллионов пользователей[2]. Согласно сведениям экспертов, в случае успешной атаки крупные компании теряют около 20 млн руб. по причине вынужденного простоя, упущенной прибыли и расходов на дополнительные услуги специалистов, предприятия среднего и малого бизнеса — в среднем 780 тыс. руб.[3]

В 2016 г. зафиксирован первый случай хищения средств с корреспондентского счета банка в Банке России, в результате чего у Русского международного банка была похищена годовая прибыль в размере более полумиллиарда рублей[4].

Прогнозируя с учетом мнения научного и экспертного сообществ тенденции развития киберпреступности в 2017 г. и в последующие годы, следует ожидать в России, как и в других странах, роста количества таких преступлений, в том числе компьютерных атак на правительственные сайты, сайты государственных и муниципальных учреждений, а также сайты средств массовой информации для продвижения различных социальных и политических идей. Кроме того, полагаем, увеличится количество кибератак на банкоматы, банки и финансово-кредитные организации; продолжится рост количества заражений мобильных устройств и терминалов для приема к оплате по пластиковым картам.

В принятом в 2013 г. российском документе «Основы государственной политики в области международной информационной безопасности на период до 2020 года» (утв. Президентом РФ 24.07.2013 № Пр-1753) дано определение *международной информационной безопасности* как такого состояния 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.

Под *системой международной информационной безопасности*, необходимой для оказания противодействия угрозам стратегической стабильности и обеспечения равноправного стратегического партнерства в глобальном информационном пространстве понимается совокупность международных и национальных институтов, призванных регулировать деятельность различных субъектов глобального информационного пространства (Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года).

К триаде угроз, связанных с применением информационного оружия, во-первых, в военно-политических целях для осуществления враждебных действий и актов агрессии, во-вторых, в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры и, в-третьих, для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ, Основы государственной политики в области международной информационной безопасности на период до 2020 года добавили опасность вмешательства во внутренние дела суверенного государства посредством информационно-коммуникационных технологий, нарушение общественной стабильности, разжигание межэтнической, межнациональной розни.

Неоднократно подчеркиваемая во многих научных исследованиях негативная субсидиарная роль киберпреступности к механизмам распространения и обработки информации свидетельствует не только о масштабных деструктивных последствиях для государства и общества, но также выступает значимым индикатором уровня и состояния правового регулирования общественных отношений, социального управления и эффективности регулирования оборота информации в целом.

В связи с активным развитием информационно-коммуникационных технологий увеличивается количество криминальных посягательств в указанной сфере, которые с каждым годом принимают новые формы. Перечень преступлений, при совершении которых используются современные информационно-коммуникационные технологии, стремительно расширяется, не только создавая угрозу причинения имущественного ущерба, но и посягая на права

[2] Развитие информационных угроз в первом квартале 2017 года: статистика // https://securelist.ru/30657/it- threat-evolution-q J-2017-statistics/ (дата обращения: 20.07.2017).

[3] Так ли страшен Интернет. О настоящей опасности киберугроз // http://www.gazeta.ru/tech/2014/11/05_a_6289085.shtml (дата обращения: 20.07.2017); Лаборатория Касперского. Информационная безопасность бизнеса 2016 // http://media.kaspersky.com/pdf/ IT_risk_report_Russia_2016.pdf (дата обращения: 20.07.2017).

[4] С корсчета Центробанка хакеры украли более 500 млн руб. // http://rg.ru/2016/05/04/s-korscheta-centrobanka-hakery-ukrali-bolee-500-mln-rublej.html (дата обращения: 20.07.2017).

личности и национальную безопасность[5].

Особое место среди субъектов противодействия распространению в сети Интернет информации, оборот которой ограничен в Российской Федерации, отводится органам прокуратуры РФ, которые не только осуществляют надзор за исполнением законов на всей территории России, но и непосредственно проводят работу по устранению причин и условий, способствовавших совершению киберпреступлений. Например, прокуроры обращаются в суд с иском о запрещении доступа к сайтам, распространяющим информацию, оборот которой на территории Российской Федерации ограничен. Так, в 2016 г. по инициативе Генеральной прокуратуры РФ заблокирован доступ к 1,2 тыс. интернет-ресурсам, посредством которых распространялись призывы к террористической деятельности; с 18,5 тыс. сайтов удалена информация экстремистского характера[6].

Информационно-телекоммуникационные сети, включая сеть Интернет, стали основным средством коммуникации для киберпреступников, которые используются ими для привлечения в свои ряды новых членов, организации совершения киберпреступлений, обмена криминальным опытом.

В системе мер борьбы с названными угрозами особую значимость приобретает задача информационного противодействия распространению информации, оборот которой ограничен или запрещен на территории Российской Федерации. Например, установлены обязанности организаторов распространения информации: хранить информацию на территории России о переданных пользователями сообщениях в течение года (с июля 2018 г. — в течение полугода); передавать правоохранительным органам ключи для расшифровки сообщений[7]. В июле 2017 г. законодательно запрещены технологии обхода блокировки информационных ресурсов[8].

Высокотехнологичные способы и характеристика криминального пространства совершения преступлений в сфере компьютерной информации определяют их результативность. Легкодоступность распространения, поиска, доступа к компьютерной информации, а также совершения криминальных манипуляций с нею, в том числе посредством неправомерного доступа к охраняемой законом информации и использования компьютерных вредоносных программ, обуславливает актуальность и востребованность научных исследований в данной сфере[9]. Вместе с тем, выявление, расследование и раскрытие преступлений в сфере компьютерной информации специфично в силу необходимости применения нестандартных решений в области правоприменения, характеристике которых, на наш взгляд, уделяется недостаточно внимания.

Факторы, осложняющие выявление, раскрытие и расследование преступлений в сфере компьютерной информации[10]:

— трансграничность сетей передачи данных и связанная с ней проблема определения национальных юрисдикций: вопрос о соотношении места совершения криминальных манипуляций с компьютерной информацией с местом фактического причинения ущерба, при этом местонахождение «цифровых» следов преступления может не совпадать ни с местом нахождения преступника при совершении преступления, ни с местом нахождения потерпевшего;

— экстенсивный характер развития новых технологий предъявляет повышенные требования к уровню квалификации и компетенции, как сотрудников правоохранительных органов, так и прокуроров, осуществляющих надзор за исполнением законов, в том числе на досудебных стадиях производства по уголовным делам;

— изменчивость как основное свойство компьютерной информации осложняет закрепление «цифровых» следов совершения преступлений и предъявляет особые требования к процедуре производства процессуальных действий, в том числе проведения судебных экспертиз;

— интервенция «информационного элемента» в сферу нормативного регулирования уголовно-процессуальных отношений само по себе выступает дестабилизирующим фактором, а именно фрагментарное включение новых норм в условиях отсутствия системного информационного законодательства.

[5] Малышенко Д. Г. Уголовная ответственность за неправомерный доступ к компьютерной информации: дисс. … канд. юрид. наук. М., 2002. С. 63.

[6] Доклад Генерального прокурора РФ Чайки Ю. Я. на заседании Совета Федерации Федерального Собрания РФ. 26.04.2017 // https://genproc.gov.ru/smi/news/genproc/news-1186517/ (дата обращения: 20.07.2017).

[7] Федеральный закон от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон "О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».

[8] Федеральный закон от 29.07.2017 № 276-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации"».

[9] Малыковцев М. М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ: дисс. … канд. юрид. наук. М., 2006. С. 108.

[10] Теоретические основы предупреждения преступности на современном этапе развития российского общества / Под общ. ред. Р. В. Жубрина. М.: Проспект, 2016. С. 398-407.

В отношении последнего отметим, что попытки законодательного регулирования использования отдельных информационных технологий ведут к утрате актуальности законопроектов еще на стадии их обсуждения в законодательном органе, так как научно-технический прогресс стремительно опережает законодателя.

Наиболее приемлемым способом преодоления сложившейся ситуации выступает формулирование универсальных международных принципов, регулирующих правила поведения людей и использование ими информационных технологий. Однако это осложнено отсутствием единой позиции государств в данном вопросе и разным уровнем проникновения информационных технологий. В современном мире отсутствуют международные соглашения, воспринятые всеми государствами, устанавливающими уголовную ответственность за преступления в сфере компьютерной информации. В регулировании отношений, связанных с установлением ответственности за компьютерные преступления, играют роль значительное количество международных межправительственных, коммерческих и общественных организаций, среди которых следует выделить ICANN и Международный союз электросвязи, которые по целям своей деятельности осуществляют лишь регулирование технических стандартов передачи, хранения и обработки информации, однако анализ их рекомендаций и установлений позволяет сделать вывод, что они оказывают существенное влияние на правоотношения.

Понимая характер возможных угроз, Российская Федерация еще в 1998 г. выступила с инициативой принятия проекта резолюции об угрозах в информационном пространстве[11] на сессии Генеральной Ассамблеи ООН, призывая к объединению усилий для противодействия использованию информационно-коммуникационных технологий в противоправных военно-политических, террористических и иных преступных целях.

Одним из первых шагов к построению подобной системы стало внесение государствами — членами Шанхайской организации сотрудничества в сентябре 2011 г. в качестве официального документа 66-й сессии Генеральной Ассамблеи ООН Правил поведения в области обеспечения международной информационной безопасности.

В 2016-2017 гг. по инициативе Российской Федерации в рамках Группы правительственных экспертов ООН было предложено вновь выработать доклад, основу которого составили бы Правила ответственного поведения государств в информационном пространстве в контексте международной безопасности с целью последующего внесения предложения о принятии Генеральной Ассамблеей ООН резолюции, закрепляющей эти Правила. Но данная инициатива была заблокирована группой западных стран. В связи с указанным важной представляется деятельность органов прокуратуры по координации международного сотрудничества между правоохранительными органами при выявлении и расследовании преступлений в сфере компьютерной информации.

Российские подходы в отношении упомянутых правил поведения основываются на следующих постулатах:

— информационно-коммуникационные технологии должны использоваться исключительно в мирных целях;

— с учетом уникальных особенностей информационного пространства наряду с применимыми к сфере их использования нормами международного права и имеющими важное значение для поддержания международного мира, безопасности и стабильности и создания открытого, безопасного, стабильного, доступного и мирного информационного пространства, могут вырабатываться дополнительные правовые нормы для регулирования международных отношений в сфере их использования;

— государства должны обладать суверенитетом над информационно-телекоммуникационной инфраструктурой на своей территории;

— государства не должны допускать возможности использования своей территории для осуществления компьютерных атак и содействовать использованию в этих целях посредников;

— государства должны бороться с внедрением и использованием скрытых вредоносных функций и программных уязвимостей, а также добиваться безопасности для пользователей.

Другим способом преодоления коллизии между усилиями отечественного законодателя и опережающими его темпами научно-технического прогресса является реализация предложения о создании кодифицированного нормативного правового акта в форме федерального закона — Информационного кодекса Российской Федерации. К сожалению, отечественная система норм, регулирующих информационные отношения, представлена многочисленными и разрозненными нормативными правовыми актами, что осложняет правоприменительную практику и обеспечение принципа неизбежности привлечения к ответственности лиц, виновных в совершении преступлений.

[11] Проект резолюции ГА ООН 53/70 от 04.12.1998 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», внесен Российской Федерацией на рассмотрение Первого комитета Главной Ассамблеи ООН (резолюция была принята без голосования).

В настоящее время в России реализуется комплекс мер, направленных на нормативное регулирование использования процессуальных документов в электронной форме в целях ускорения взаимодействия участников уголовного судопроизводства и сокращения сроков уголовного судопроизводства: вещественными доказательствами по уголовным делам служат электронные носители информации, содержащие электронные документы; введены отдельные элементы электронного документооборота[12].

Сложности возникают в связи с отсутствием общепризнанного международного стандарта построения системы электронных документов, образующих уголовное дело. Несмотря на то, что технические решения данной проблемы уже реализованы на практике, они носят разобщенный характер и не связаны едиными стандартами представления и хранения информации.

В качестве положительного опыта России следует отметить функционирование в Генеральной прокуратуре РФ внутренней информационной системы всех органов прокуратуры. Это позволяет предположить и возможность формирования единой информационной системы, объединяющей все правоохранительные органы и суд в рамках уголовного процесса[13]. Другой высокотехнологичный проект — государственная автоматизированная система «Правовая статистика». Запланировано создание специального сервиса, доступного в том числе на мобильных устройствах, с помощью которого каждый гражданин сможет подать заявление о преступлении в правоохранительные органы в электронном виде. Этот документ сразу же будет занесен в систему правовой статистики и зарегистрирован, после чего автоматически направится по подследственности. При этом автор обращения сможет навести справку о статусе своего заявления[14].

Вовлечение «информационного элемента» в орбиту уголовно-правовых отношений требует совершенствования уголовно-процессуального законодательства в части регламентации процессуальных действий в отношении компьютерной информации. Считаем целесообразным:

— практическую реализацию организационных мер, а именно, разработку межведомственного нормативного акта по вопросам выявления, пресечения, расследования и предупреждения преступлений данной категории;

—разработку разъяснений Верховного Суда РФ по вопросам квалификации и определению наказаний за компьютерные преступления;

— усиление уголовной ответственности за преступления, совершенные с использованием современных информационно-телекоммуникационных технологий, конкретизацию составов преступлений, расширение перечня объектов уголовно-правовой охраны;

— внесение в уголовное, гражданское и административное законодательство положений об оценке ущерба, причиненного компьютерными правонарушениями, критериях, которыми должны руководствоваться правоохранительные органы и суд при определении размера этого ущерба и его возмещении виновными;

—внесение в уголовно-процессуальное законодательство положений: конкретизирующих статус цифровых доказательств; определяющих особенности выполнения дистанционных следственных действий; устанавливающих обязательность участия специалиста при изъятии цифровых следов; регламентирующих особенности осуществления электронного документооборота в рамках уголовного судопроизводства; конкретизирующих процессуальные полномочия специалиста-представителя коммерческой организации, предоставляющей услуги информационной безопасности (осуществляющих дистанционный поиск и закрепление «цифровых» следов преступлений, в том числе изъятие данных из DLP систем для последующего предоставления в правоохранительные органы; осуществляющих судебные экспертизы, и т.д.), что по существу вступает в конкуренцию с функциями органов предварительного следствия и дознания, обладает признаками проведения отдельных следственных действий и оперативно-розыскных мероприятий;

—дополнение информационного законодательства и Федерального закона «О прокуратуре Российской Федерации» положениями, расширяющими полномочия прокуроров по внесудебному ограничению доступа к компьютерной информации, оборот которой запрещен либо ограничен на территории Российской Федерации;

— развитие международного сотрудничества посредством соглашений об обеспечении информационной безопасности;

— участие в международных конвенциях и договорах по борьбе с международной киберпреступностью;

---

[12] См. подробнее: Федеральный закон от 03.07.2016 № 323-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации по вопросам совершенствования оснований и порядка освобождения от уголовной ответственности»; Федеральный закон от 23.06.2016 № 220-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти».

[13] Инсаров О. А. Электронная подпись прокурора // Прокурор. 2015. № 4. С. 35—38.

[14] Интервью Генерального прокурора РФ Чайки Ю. Я. газете «Известия» // https://genproc.gov.ru/smi/news/genproc/news-1187391/ (дата обращения: 20.07.2017).

— оказание всестороннего содействия в вопросах уголовного преследования лиц, имеющих отношение к финансированию или поддержке киберпреступлений;

— заморозку банковских средств и других финансовых активов и экономических ресурсов лиц, которые пытаются совершить или совершают киберпреступления;

— создание международного банка данных криминалистической информации о киберпреступлениях и лицах, их совершающих (банк данных о хакерах);

— повышение скорости обмена оперативной информацией о любых действиях киберпреступных групп, торговле специальным программным обеспечением и вычислительным оборудованием, распространении вредоносных компьютерных программ и технической информации об уязвимостях программного обеспечения.

Несмотря на то, что в настоящее время широкое распространение получили относительно эффективные меры предупреждения преступлений в сфере компьютерной информации, находящиеся в плоскости применения программных средств защиты компьютерной информации, необходима реализация имеющегося потенциала в части формирования навыков соблюдения элементарной информационной безопасности в целях предупреждения совершения преступлений в сфере компьютерной информации, в том числе в информационно-телекоммуникационных сетях, и своевременного возмещения ущерба в результате совершения подобных преступлений.

Прокуратура РФ осуществляет координацию деятельности правоохранительных органов по противодействию преступлениям, в том числе в сфере компьютерной информации, поэтому обоснованным представляется создание ситуационного центра при прокуратуре РФ с функциями обмена информацией о фактах совершения подобных преступлений с международными и межгосударственными (Интерпол, Финцерт), зарубежными правоохранительными органами и коммерческими организациями (например, банковские организации, крупные телекоммуникационные компании, разработчики антивирусного программного обеспечения и т.д.), с отечественными организациями, заинтересованными в сотрудничестве и оперативном обмене информацией.

Необходимо создать специализированный государственный фонд для компенсации ущерба потерпевшим от преступлений в сфере компьютерной информации, в том случае, если фактически в силу юрисдикционных коллизий невозможно установить лиц, совершивших подобные преступления, а граждане Российской Федерации в большинстве случаев не обладают возможностями по обращению в правоохранительные органы иностранных государств и последующей защите собственных интересов на территории иностранных государств.

Список литературы

1. Инсаров О.А. Электронная подпись прокурора // Прокурор. 2015. № 4. С. 35—38.
2. Лаборатория Касперского. Информационная безопасность бизнеса 2016 // http://media.kaspersky.com/pdf/IT_risk_report_Russia_2016.pdf (дата обращения: 20.07.2017).
3. Малыковцев М.М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ: дисс. … канд. юрид. наук. М., 2006. С. 108.
4. Малышенко Д.Г. Уголовная ответственность за неправомерный доступ к компьютерной информации: дисс. … канд. юрид. наук. М., 2002. С. 63.
5. Теоретические основы предупреждения преступности на современном этапе развития российского общества / Под общ. ред. Р.В. Жубрина. М.: Проспект, 2016. С. 398-407.

Aspects of Information Security of the Russian Federation

Khaliullin A.I.,
Scientific Employee of the Scientific Research Institute
of the Academy of the Prosecutor General's Office of the RF
E-mail: adel@lenta.ru

Abstract. *The scientific article considers issues of ensuring international information security, the component of which is the information security of the Russian Federation. High-tech methods and characteristics of the criminal space for committing crimes in the field of computer information determine their effectiveness. At the same time, there is no common position of states in the issues of countering cybercrime, which is predetermined, among other things, by the different level of penetration of information technologies. Despite the efforts of the Russian Federation to formulate rules for networking, including the inadmissibility of violating the information (network)*

sovereignty of states and other proposals put on the agenda of working groups at the UN, they do not find support from individual groups of countries. The absence of universally recognized borders in the network space, as well as procedures for interaction between law enforcement agencies in order to counteract cybercrime, forms a potentially conflicting information environment with a relatively low level of security. Identifying, suppressing and investigating cybercrime is, in most cases, complicated by the transboundary nature of the acts committed, which involves coordinating the efforts of law enforcement agencies of different states.

Currently Russia is implementing a set of measures aimed at the regulatory regulation of the use of procedural documents in electronic form in order to accelerate the interaction of participants in criminal proceedings and reduce the terms of criminal proceedings: material evidence in criminal cases is electronic media containing electronic documents; separate elements of electronic document management are introduced. However, the legislation of the Russian Federation in the information sphere, as well as the practice of its application, needs further improvement.

A special place among the subjects of counteracting the dissemination of information on the Internet, the circulation of which is limited in the territory of the Russian Federation, is assigned to the bodies of the Procurator's Office of the Russian Federation, which not only oversees the implementation of laws throughout Russia, but also directly eliminates the causes and conditions that contributed to the commission of cybercrime.

***Keywords**: information security, cybercrime, informatization, prosecutor's supervision, criminal justice, jurisdiction.*

References

1. Insarov O. A. Elektronnaya podpis prokurora // Prokuror. 2015. № 4. S. 35-38.
2. Laboratoriya Kasperskogo. Informatsionnaya bezopasnost biznesa 2016 // http://media.kaspersky.com/pdf/IT_risk_report_Russia_2016.pdf (data obrascheniya: 20.07.2017).
3. Malykovtsev M. M. Ugolovnaya otvetstvennost za sozdanie, ispolzovanie i rasprostranenie vredonosnykh programm dlya EVM: diss. … kand. yurid. nauk. M., 2006. S. 108.
4. Malyshenko D. G. Ugolovnaya otvetstvennost za nepravomernyj dostup k kompyuternoj informatsii: diss. … kand. yurid. nauk. M., 2002. S. 63.
5. Teoreticheskie osnovy preduprezhdeniya prestupnosti na sovremennom etape razvitiya rossijskogo obschestva / Pod obsch. red. R. V. Zhubrina. M.: Prospekt, 2016. S. 398-407.