УДК 343.9
DOI 10.17150/1996-7756.2015.9(1).101-110

ПОЛИТИЧЕСКИЕ ПРИЧИНЫ КАК СОВРЕМЕННЫЕ ФАКТОРЫ ЭВОЛЮЦИИ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Д.А. Липинский[1], К.Н. Евдокимов[2]
[1] Тольяттинский государственный университет, г. Тольятти, Российская Федерация
[2] Иркутский юридический институт (филиал) Академии Генеральной прокуратуры РФ, г. Иркутск, Российская Федерация

Информация о статье
Дата поступления
5 ноября 2014 г.

Дата принятия в печать
4 февраля 2015 г.

Дата онлайн-размещения
31 марта 2015 г.

Ключевые слова
Компьютерная преступность; преступления в сфере компьютерной информации; киберпреступность; кибероружие; кибершпионаж; причины и факторы компьютерной преступности

Аннотация. Актуальность данного научного исследования обусловлена тем, что за последние годы компьютерная преступность в Российской Федерации трансформировалась, приобретя организованный, «профессиональный» и экономически направленный характер. Целью научной статьи является анализ политической составляющей причинного комплекса совершения компьютерных преступлений в России.

По мнению авторов, к числу наиболее значимых политических причин, определяющих развитие компьютерной преступности в Российской Федерации, следует отнести: 1) развитие хактивизма как политического движения против государственного контроля в глобальной информационной сети Интернет и за соблюдение государством информационных прав человека; 2) причинение вреда государственным интересам Российской Федерации, создание помех для функционирования механизма государственной власти в России со стороны вооруженных сил враждебных стран путем использования ими вредоносных компьютерных программ в качестве информационного оружия; 3) деятельность спецслужб иностранных государств в отношении российских органов власти, учреждений, предприятий для получения информации геополитического, военно-технического, дипломатического и иного стратегического характера, т.е. кибершпионаж.

Для более эффективного противодействия преступлениям в сфере компьютерной информации авторы предлагают дополнить диспозиции ч. 3 ст. 272, ч. 2 ст. 273, ч. 1 ст. 274 УК РФ новым квалифицирующим признаком: «Те же деяния, совершенные с целью устрашения населения или воздействия на принятие решения органами государственной власти и (или) местного самоуправления, а также воспрепятствования нормальной деятельности средств массовой информации, органов государственной власти и местного самоуправления, государственных и муниципальных учреждений, предприятий», установив санкцию до десяти лет лишения свободы. При этом авторы полагают необходимым внести изменения в ст. 151 УПК РФ и отнести преступления, предусмотренные ч. 2–4 ст. 272, ч. 2, 3 ст. 273, ч. 1, 2 ст. 274 УК РФ к подследственности органов ФСБ РФ.

POLITICAL REASONS AS MODERN FACTORS OF THE EVOLUTION OF COMPUTER CRIMES IN THE RUSSIAN FEDERATION

Lipinsky, Dmitry A.[1], Evdokimov, Konstantin N.[2]
[1] Togliatti state University, Togliatti, Russian Federation
[2] Irkutsk Law Institute (Branch) of the Academy of the General Prosecutor's Office of the Russian Federation, Irkutsk, Russian Federation

Article info
Received
2014 November 5

Accepted
2015 February 4

Available online
2015 March 31

Abstract. The relevance of this research is stipulated by the fact that, in recent years, computer crime in the Russian Federation has been transformed, and has become organized, professional and economically oriented by its nature. The purpose of this scientific article is to analyze political component of the causal complex of committing computer crimes in Russia.

According to the authors, among the most important political factors determining the development of computer crime in the Russian Federation, there are: 1) development of the hacktivist movement as a political protest movement against state control in the

ISSN 1996-7756

Keywords
Computer crime; crimes in the sphere of computer information; cybercrime; cyber weapons; cyber espionage; reasons and factors of computer crime

global information network «Internet» and compliance with the state information of human rights; 2) the harm to the public interest, to the activities of the mechanism of state power of the Russian Federation by armed forces of hostile countries, by use of malicious computer programs as information weapons; 3) the activities of secret services of foreign States in respect of the Russian authorities, institutions, enterprises involved with the information of geopolitical, military-technical, diplomatic and otherwise strategically oriented ones, i.e. the «cyber espionage».
To more effectively combat crimes in the sphere of computer information, the authors propose to amend the disposition by parts 3 article 272; by parts 2 article 273; by parts 1 article 274 of the Criminal Code of the Russian Federation by a new qualifying characteristic: «The same acts, committed with the purpose of intimidating a population or impact on decision-making by public authorities and/or local governments, as well as impeding the normal functioning of the media, public authorities and local self-government, state and municipal institutions, enterprises», imposing a sanction of up to 10 years imprisonment.
For this purpose, the authors believe it necessary to make changes in article 151 of the Code and to include crimes under the Criminal Code of the RF provisioned by parts 2–4 article 272; by parts 2, 3 article 273; by parts 1, 2 article 274 of the Criminal Code of the Russian Federation to the investigative jurisdiction of the FSB.

Проблеме компьютерной преступности в Российской Федерации, причинам ее возникновения и развития отечественные ученые и правоприменители в последние годы уделяют пристальное внимание.

Тотальное применение информационных технологий в банковской, торговой, промышленной, научной, образовательной, культурной и других сферах общественной жизни, а также широкое использование компьютерной техники, электронно-цифровых баз данных, информационно-телекоммуникационных систем в области управления детерминируют существование компьютерной преступности и ее качественное развитие в современной России.

За прошедшие годы компьютерная преступность в нашей стране значительно трансформировалась, приобретя по сравнению с 1990-ми гг. более организованный, «профессиональный» и экономически направленный характер. При этом вред, причиняемый российскому обществу преступлениями в сфере компьютерной информации, имеет колоссальный масштаб.

Так, по оценкам аналитиков компании Group-IB, объем рынка киберпреступности в РФ в 2012 г. составил 1,93 млрд дол. [22]. В свою очередь, американская корпорация Symantec оценила ущерб от киберпреступности в России за 2013 г. в 1 млрд дол., а за 2012 г. — в 1,48 млрд. Между тем общий ущерб от киберпреступности в мире в 2013 г. составил 113 млрд дол. против 110 млрд дол. в 2012 г. [24].

Как мы видим, данные аналитиков разнятся, однако, по мнению авторов, это вполне объяснимо высоким уровнем латентности компьютерных преступлений, а также отсутствием единой международной методики расчета вреда, причиненного киберпреступниками.

Согласно официальной статистике ГИАЦ МВД РФ, за последние годы в России были возбуждены уголовные дела по таким видам преступлений в сфере компьютерной информации, как неправомерный доступ к компьютерной информации (ст. 272 УК РФ) (в 2010 г. — 6 132, в 2011 г. — 2 005, в 2012 г. — 1 930, в 2013 г. — 1 799); создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) (в 2010 г. — 1 010, в 2011 г. — 693, в 2012 г. — 889, в 2013 г. — 764); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) (в 2010 г. — 0 [10], в 2011 г. — 0 [11], в 2012 г. — 1 [12], в 2013 г. — 0 [9]).

Из приведенных статистических данных очевидно, что среди преступлений в сфере компьютерной информации преобладают неправомерный доступ к компьютерной информации (ст. 272 УК РФ), а также создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ), при этом отмечается общее снижение числа регистрируемых преступлений в данной сфере. Это не может не вызывать вопросы и, наверное, определенную обеспокоенность у специалистов в области информационной безопасности по поводу того, насколько реально официальная статистика отражает масштабы существующей

ISSN 1996-7756

компьютерной преступности, поскольку, например, в 2012 г. при возбужденных 889 уголовных делах по факту создания, использования и распространения вредоносных компьютерных программ только компанией по производству антивирусного программного обеспечения «Лаборатория Касперского» в России было зафиксировано 317 697 806 вирусных атак (2-е место в мире после США) [16]. Это фактически миллионы потенциальных уголовных дел, так как состав преступления, предусмотренный ч. 1 ст. 273 УК РФ, является по конструкции формальным и не предусматривает обязательного наступления вреда, достаточно лишь факта создания, использования или распространения вредоносной компьютерной программы, т.е. в данном случае — факта вирусной атаки на компьютер и находящуюся на нем информацию.

Однако цель настоящей научной статьи не исследование экономических, технических, организационных, кадровых и иных причин российской компьютерной преступности, а анализ политической составляющей ее причинного комплекса.

Прежде чем перейти к рассмотрению политических причин компьютерной преступности, необходимо определиться с используемой юридической терминологией.

Так, под компьютерной преступностью чаще всего понимается совокупность преступлений, в которых предметом преступных посягательств выступает компьютерная информация [7, с. 830].

В свою очередь, киберпреступность — это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству в рамках компьютерных систем или сетей и против компьютерных систем, компьютерных сетей и компьютерных данных [8, с. 48].

При этом авторы «модельного закона» о киберпреступности (2009) Международного союза электросвязи определяют киберпространство как «физическое и нефизическое пространство, созданное и (или) сформированное следующим образом: компьютеры, компьютерные системы, сети, их компьютерные программы, компьютерные данные, данные контента, движение данных и пользователи» [18].

К настоящему времени в отечественной криминологической науке сложилось два подхода к соотношению понятий «компьютерная преступность» и «киберпреступность». Первый предусматривает отождествление данных терминов [14, с. 1], представители второго подхода считают, что понятие «киберпреступность» по своему смыслу и содержанию шире понятия «компьютерная преступность», объясняя это тем, что киберпреступления совершаются не только с помощью компьютеров и в отношении компьютерной информации, но и с помощью самой компьютерной информации, глобальной информационной сети Интернет и иных информационно-телекоммуникационных сетей, а также других средств хранения, обработки, передачи электронно-цифровой информации (айпады, айфоны, коммуникаторы, смартфоны, оптоволоконные системы связи и т.д.), не являющихся компьютерами в нашем понимании.

Авторы данной статьи придерживаются точки зрения второй группы ученых [8; 15], считая понятие «киберпреступность» шире по объему и содержанию, чем понятие «компьютерная преступность», так как оно по сравнению с последним носит более глобальный и всеохватывающий характер. При этом авторы полагают, что понятия «компьютерные преступления» и «преступления в сфере компьютерной информации» также неравнозначны и соотносятся между собой как родовое и видовое понятия, где преступления в сфере компьютерной информации выступают только разновидностью компьютерных преступлений. Последнее, на наш взгляд, обусловлено тем, что законодатель в гл. 28 УК РФ объединил все преступные деяния, где предметом преступного посягательства является компьютерная информация и непосредственным объектом состава преступления выступают общественные отношения в сфере безопасного хранения, обработки и передачи компьютерной информации, дав им название «преступления в сфере компьютерной информации».

При этом понятие «компьютерные преступления», по нашему мнению, также шире по своему значению и включает в себя не только преступления, предусмотренные ст. 272–274 УК РФ, где предметом преступного посягательства выступает компьютерная информация, но и преступления, где компьютерная информация служит средством совершения преступного деяния, а непосредственный объект состава преступления может включать в себя и другие

ISSN 1996-7756

общественные отношения, например отношения в сфере собственности. Это позволяет отнести к компьютерным преступлениям такие деяния, как мошенничество с использованием платежных карт (ст. 159.3 УК РФ) и мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ). Данный подход преобладает в уголовном законодательстве большинства европейских стран, ратифицировавших Европейскую конвенцию о киберпреступности [5].

Однако, возвращаясь к причинам российской компьютерной преступности и понимая невозможность в рамках отдельной научной статьи рассмотреть всю проблематику, затрагивающую данную тему, авторы сконцентрировались на вопросе о причинах компьютерной преступности, а также на необходимости исследовать политическую составляющую причинного комплекса данного вида преступности. Проведенный анализ научной литературы позволил получить следующие ответы на интересующий вопрос.

По мнению Ю. Гульбина, одной из основных причин возникновения компьютерной преступности стало информационно-технологическое перевооружение предприятий, учреждений и организаций, насыщение их компьютерной техникой, программным обеспечением, базами данных, другой — реальная возможность получения значительной экономической выгоды от противоправных деяний с использованием ЭВМ. Появилась заманчивая перспектива как бы обменивать продукт своих неправомерных действий на иные материальные ценности [3, с. 24].

В свою очередь, В.Б. Вехов считает, что основными причинами и условиями, способствующими совершению компьютерных преступлений, главным образом стали:

– неконтролируемый доступ сотрудников к пульту управления (клавиатуре) компьютера, используемого как автономно, так и в качестве рабочей станции автоматизированной сети для дистанционной передачи данных первичных бухгалтерских документов в процессе финансовых операций;

– бесконтрольность действий обслуживающего персонала, что позволяет преступнику свободно использовать указанную в предыдущем пункте ЭВМ в качестве орудия совершения преступления;

– низкий уровень программного обеспечения, которое не имеет контрольной защиты, обеспечивающей проверку соответствия и правильности вводимой информации;

– несовершенство парольной системы защиты от несанкционированного доступа к рабочей станции и ее программному обеспечению, которая не обеспечивает достоверную идентификацию пользователя по индивидуальным биометрическим параметрам;

– отсутствие должностного лица, отвечающего за режим секретности и конфиденциальности коммерческой информации и ее безопасность в части защиты средств компьютерной техники от несанкционированного доступа;

– отсутствие категорирования (разграничения) допуска сотрудников к документации строгой финансовой отчетности, в том числе в форме машинной информации;

– отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной конфиденциальной информации [2, с. 114].

Между тем У.В. Зинина в качестве причин совершения преступлений в сфере компьютерной информации указывает то, что «системы защиты информационных систем и сетей связи не успевают совершенствоваться вслед за все более совершенными методами и способами совершения преступлений в сфере компьютерной информации. Сюда же можно отнести и не всегда серьезный подход руководителей предприятий к вопросу обеспечения информационной безопасности и защите информации, а нередко даже и сокрытие от правоохранительных органов фактов компьютерного преступления в организации» [4, с. 18]. Таким образом, У.В. Зинина делает акцент на технических и организационных причинах совершения преступлений в сфере компьютерной информации.

Интересной, на наш взгляд, является позиция В.А. Бессонова, который считает, что компьютерные технологии непроизвольно формируют, возбуждают, вызывают у преступника «чувство уязвимости любой защиты», в свою очередь, у человека-жертвы всегда присутствует особое антропологическое свойство — криминальная уязвимость, а следовательно, у компьютера, хранящего в себе массу ценной информации, присутствует также особое свойство — «компьютерная» уязвимость. Таким образом, «компьютерная» уязвимость подразуме-

ISSN 1996-7756

вает способность персонального компьютера в силу его технических, потребительских свойств быть виктимным. При этом виктимологические факторы, влияющие на совершение компьютерных преступлений, делятся по содержанию на социальные, поведенческие и нравственно-психологические [1, с. 211].

Можно согласиться с А.Н. Копырюлиным, который полагает, что «специфические факторы, способствующие совершению преступлений в сфере компьютерной информации, относятся к социально-экономической, правовой и организационно-управленческим сферам» [6, с. 19].

Вместе с тем, не отрицая приведенные научные точки зрения, авторы считают, что причинный комплекс компьютерной преступности становится все более разнообразным, что обусловлено продолжающимся развитием информационных технологий и крупномасштабным использованием их в политической сфере жизни современного общества. Поэтому наряду с причинами компьютерной преступности юридического, социально-экономического, организационно-технического, кадрового и иного характера в сфере информационной безопасности все более активно заявляют о себе причины политической направленности.

Политические причины совершения преступлений в сфере компьютерной информации до недавнего времени не выделялись в качестве значимых, хотя политические мотивы совершения компьютерных преступлений теоретически допускались некоторыми учеными [2, с. 41].

На данный момент ситуация кардинально изменилась, и, по нашему мнению, при анализе причинного комплекса компьютерной преступности в России можно с уверенностью говорить о наличии следующих причин политического характера.

Во-первых, это возникновение и развитие хактивизма как политического движения против государственного контроля в глобальной информационной сети Интернет и за соблюдение государством информационных прав человека.

Хактивизм (hacktivism, от англ. hack — рубить и acktivism — активизм) предусматривает борьбу за права и свободы личности (свобода слова, свобода информации и т.д.) посредством использования компьютерных технологий и информационно-телекоммуникационных сетей, включая сеть Интернет. Наиболее известные международные хактивистские движения — WikiLeaks и Anonymous. Считается, что термин был придуман в США (штат Техас) в 1996 г. членом организации Cult of the Dead Cow («Культ мертвой коровы») под именем Omega [28].

Протестной формой хактивистского движения является гражданское неповиновение в виде блокирования правительственных вебсайтов, перенаправления URL, совершения DDoS-атак, краж компьютерной информации и демпинга, создание сайтов-пародий и т.д.

Например, российские хакеры из группы Anonymous в марте — мае 2012 г. предприняли DDoS-атаки против сайтов СМИ «Дождь», НТВ, «Коммерсантъ», Slon.ru, «Эхо Москвы», а также сайтов президента и правительства РФ, заблокировав их на достаточно продолжительное время. Как результат, в январе 2013 г. УФСБ РФ по Красноярскому краю направило в суд уголовные дела в отношении двух жителей г. Красноярска, граждан С. и Х., которые 6, 7 и 9 мая 2012 г. при помощи вредоносных компьютерных программ осуществили DDoS-атаки на сайты президента и правительства РФ, временно блокировав их. Действия обвиняемых были квалифицированы по ч. 1 ст. 273 УК РФ, т.е. создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации [25].

Таким образом, хактивистское движение, несмотря на свою политическую направленность и благородную цель — «обеспечить свободу информации», без стеснения использует вредоносные компьютерные программы, осуществляя взломы сайтов средств массовой информации, государственных учреждений и органов власти либо с применением уже известного вредоносного программного обеспечения, либо привлекая к сотрудничеству вирусописателей для получения от них новых компьютерных вирусов.

Во-вторых, политической причиной компьютерной преступности в России выступает то, что вооруженные силы и спецслужбы враждебных стран стремятся причинить вред государственным интересам, помешать функционированию механизма государственной власти Российской Федерации путем использования

ISSN 1996-7756

вредоносных компьютерных программ в качестве информационного оружия.

Так называемое кибероружие может быть использовано в политических целях для оказания информационного давления или пропаганды путем получения контроля над электронными средствами массовой информации, киберсаботажа с целью вывода из строя средств связи и массовых коммуникаций, блокирования объектов энергоснабжения и транспортной инфраструктуры, нарушения производственной деятельности предприятий оборонно-промышленного комплекса, а также причинения вреда иным объектам стратегического значения.

Так, в частности, в сентябре 2010 г. вирус Stuxnet проник в компьютеры иранской атомной станции в Бушере и вывел из строя пятую часть центрифуг по обогащению урана, но, к счастью, он не смог вывести из строя основную операционную систему АЭС. Если бы ему это удалось, могли возникнуть катастрофические последствия [26].

Журналистское расследование газеты «Нью-Йорк таймс», проведенное в 2011 г., подтвердило предположение «Лаборатории Касперского», доказав, что вредоносная программа Stuxnet была создана спецслужбами Израиля и США для саботажа ядерной программы Ирана [30].

В апреле 2012 г. был обнаружен «таинственный» вирус-троян Wiper, в результате действия которого были уничтожены базы данных в десятках организаций Ирана, при этом больше всего пострадал крупнейший в стране нефтяной терминал, работа которого была остановлена на несколько дней из-за того, что были уничтожены данные о нефтяных контрактах. Однако не было найдено ни одного образца вредоносной программы, использованной в этих атаках, что многих заставило усомниться в точности сведений, содержащихся в сообщениях СМИ. В процессе расследования апрельской вредоносной атаки «Лаборатории Касперского» удалось получить и проанализировать образы нескольких жестких дисков, атакованных Wiper. В итоге эксперты компании подтвердили, что инциденты действительно имели место и что вредоносная программа, использованная в этих атаках, существовала в апреле 2012 г., но после активации Wiper от вредоносной программы не осталось почти никаких следов [32].

В подтверждение научных тезисов авторов можно привести публикацию газеты «Вашингтон пост» от 1 сентября 2013 г., которая со ссылкой на документы, рассекреченные экссотрудником ЦРУ Э. Сноуденом, сообщила, что разведывательные службы США в 2011 г. провели 231 кибератаку, направленную против электронных сетей иностранных государств, в том числе России, Китая, Ирана и КНДР [23].

В-третьих, политической причиной компьютерной преступности в России является кибершпионаж, осуществляемый спецслужбами иностранных государств для получения информации геополитического, военно-технического, дипломатического и иного стратегического характера.

Так, уже упоминавшейся «Лабораторией Касперского» при исследовании инцидента с вирусом Wiper была обнаружена другая вредоносная программа — Flame и, как следствие, масштабная кампания по кибершпионажу на Ближнем Востоке.

Вирус Flame стал одной из наиболее опасных киберугроз за всю историю существования вредоносного программного обеспечения. После полного его развертывания на компьютере суммарный размер входящих в его состав модулей составляет более 20 МБ. Эти модули выполняют широкий набор вредоносных функций, таких как перехват аудиоданных, сканирование устройств, подключенных по протоколу Bluetooth, кража документов и снимков экрана на зараженном компьютере, информации об использовании клавиш клавиатуры и др.

Специалисты обнаружили тесную связь между Flame и Stuxnet, и это позволило прийти к выводу, что разработчики Flame действовали в сотрудничестве с разработчиками Stuxnet, возможно, в рамках одного проекта. Самому проекту Flame не меньше пяти лет. При этом эксперты «Лаборатории Касперского» считают, что вредоносные программы Stuxnet, Wiper, Flame и Gauss, обнаруженные на Ближнем Востоке в 2010–2012 гг., несомненно являются кибероружием, разработанным при государственной поддержке [31].

Наиболее ярким фактом кибершпионажа против Российской Федерации можно считать обнаружение в 2012 г. вредоносной компьютерной программы Backdoor.Win32.Sputnik («Красный Октябрь»). В частности, 14 января 2013 г. «Лабораторией Касперского» был опубликован

ISSN 1996-7756

отчет, в котором заявлено об обнаружении вируса-трояна Backdoor.Win32.Sputnik (условное название — Red October («Красный Октябрь») по названию шпионской советской подводной лодки в одноименном американском фильме «Охота за «Красным Октябрем») и раскрытии глобальной шпионской сети. Зараженными оказались компьютерные системы организаций, относящихся к восьми категориям: правительственные структуры; дипломатические ведомства/посольства; исследовательские институты; торговые и коммерческие структуры; организации, осуществляющие ядерные/энергетические исследования; нефтяные и газовые компании; организации, принадлежащие аэрокосмической отрасли; военные ведомства и компании, связанные с созданием вооружений.

Данная шпионская сеть существует на протяжении пяти лет и в настоящий момент включает в себя зараженные компьютеры более чем 300 различных организаций из ряда стран Восточной Европы, Азии, Африки и Северной Америки. Заражение вирусом шло через электронную почту. Жертва получала письмо с предложением приобрести подержанный автомобиль Mazda-323 1998 года выпуска. После скачивания файла вредоносная программа Backdoor.Win32.Sputnik проникала в компьютерную сеть и сразу же начинала собирать информацию. При этом информация собиралась со всех подключенных к сети компьютеров, флешносителей и мобильных телефонов. Похищенные данные отправлялись на сервер хакеров, но не напрямую, а через обширную сеть серверов прикрытия (прокси-серверов).

Количество государственных организаций и учреждений, оказавшихся пораженными вирусом Backdoor.Win32.Sputnik, составило: в России — 38, Казахстане — 21, Азербайджане и Бельгии — по 15, Индии — 14, Афганистане и Армении — по 10, Иране и Туркменистане — по 7, Украине и Вьетнаме — по 6, Белоруссии, Греции, Италии, Марокко, Пакистане, Швейцарии, Уганде, Объединенных Арабских Эмиратах — по 5.

До настоящего времени создатели «Красного Октября» не выявлены, и вирус продолжает распространяться через электронную почту в информационной сети Интернет [33].

Продолжая разговор о политических причинах компьютерной преступности в современной России, можно уверенно говорить о создании в США и КНР специализированных государственных структур (условно назовем их кибервойсками), имеющих возможность применять кибероружие. При этом какая-либо информация об их структуре и деятельности носит строго засекреченный характер, но в средства массовой информации периодически просачиваются скудные сведения о деятельности кибервойск этих государств.

Так, 17 апреля 2012 г. газета «Гардиан» сообщила, что «представители военных и внешнеполитических ведомств США и КНР только в 2011 г. провели две серии штабных учений по взаимодействию на театре военных действий в киберпространстве. По информации «Гардиан», американо-китайские учения были направлены на предотвращение эскалации военных конфликтов в случаях, когда одна из сторон считает, что против нее проведена атака в киберпространстве.

В первой серии штабных игр китайские и американские военные отрабатывали ситуацию с атакой мощного компьютерного вируса, такого как Stuxnet, который вывел из строя центрифуги для обогащения урана в Иране. Участники этих игр должны были описать свои действия в случае подобной атаки.

Во второй серии совместных учений военные и дипломаты должны были описать свою реакцию в случае, если об аналогичной атаке было заведомо известно то, что она была проведена противоположной стороной. То есть китайские участники должны были описать свои действия при атаке со стороны США, а американские — в случае атаки, заведомо исходящей из КНР» [27].

Учитывая серьезность вышеуказанных политических причин компьютерной преступности и существующих киберугроз национальной безопасности РФ, Россия сделала первые шаги по защите своих интересов и суверенитета. Так, 15 января 2013 г. президент РФ издал указ № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [13], в соответствии с которым возложил на Федеральную службу безопасности Российской Федерации полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федера-

ISSN 1996-7756

ции — информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом.

На данный момент проходят правовую экспертизу проекты федеральных законов «О безопасности критической информационной инфраструктуры Российской Федерации» и «О внесении изменений в законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации», разработанные ФСБ России. Планируется, что они вступят в силу с 1 января 2015 г.

Второй законопроект устанавливает меры ответственности за нарушение законодательства о безопасности критической информационной инфраструктуры РФ. В том числе в документе закрепляется уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации, повлекший ущерб безопасности критической информационной инфраструктуры РФ или создавший угрозу его наступления (наказание — лишение свободы на срок до десяти лет).

Также предусматривается уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к таким сетям, повлекшее ущерб безопасности критической информационной инфраструктуры РФ или создавшее угрозу его наступления (наказание — до семи лет лишения свободы).

При этом в УПК РФ планируется определить прямую подследственность органов ФСБ России по составам преступлений, предусмотренных ст. 272 и 274 УК РФ.

Тексты законопроектов размещены на Едином портале раскрытия информации о подготовке федеральными органами исполнительной власти проектов нормативных правовых актов и результатах их общественного обсуждения (номера ID: 00/04-5890/08-13/20-13-4 и ID: 00/04-5892/08-13/20-13-4) [29].

С учетом вышесказанного авторы считают целесообразным учесть политические причины компьютерной преступности и дополнить диспозиции ч. 3 ст. 272, ч. 2 ст. 273, ч. 1 ст. 274 УК РФ новым квалифицирующим признаком: «Те же деяния, совершенные с целью устрашения населения или воздействия на принятие решения органами государственной власти и (или) местного самоуправления, а также воспрепятствования нормальной деятельности средств массовой информации, органов государственной власти и местного самоуправления, государственных и муниципальных учреждений, предприятий», установив санкцию до десяти лет лишения свободы. Это, по мнению авторов, справедливо с учетом повышенной общественной опасности указанных преступных деяний, которые представляют собой не что иное, как кибертерроризм, и должны наказываться более сурово.

При этом авторы полагают необходимым внести изменения в ст. 151 УПК РФ и отнести преступления, предусмотренные ч. 2–4 ст. 272, ч. 2, 3 ст. 273, ч. 1, 2 ст. 274 УК РФ к подследственности органов ФСБ РФ.

Наконец, устранение рассмотренных политических причин компьютерной преступности должно носить политический, правовой, социально-экономический, организационно-технический, т.е. комплексный характер (совершенствование законодательства, развитие российской экономики, более качественная подготовка сотрудников правоохранительных органов в сфере информационной безопасности, развитие отечественной электроники и производства программного обеспечения, привлечение талантливых программистов на государственную службу и т.д.) с использованием возможностей не только государства, но и институтов гражданского общества.

СПИСОК ЛИТЕРАТУРЫ

1. Бессонов В.А. Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации : дис. ... канд. юрид. наук : 12.00.08 / В.А. Бессонов. — Н. Новгород, 2000. — 249 с.

2. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов ; под ред. Б.П. Смагоринского. — М. : Право и закон, 1996. — 182 с.

3. Гульбин Ю. Преступления в сфере компьютерной информации / Ю. Гульбин // Российская юстиция. — 1997. — № 10. — С. 24–25.

4. Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве : автореф. дис. ... канд. юрид. наук : 12.00.08 / У.В. Зинина. — М., 2007. — 33 с.

ISSN 1996-7756

5. Конвенция о преступности в сфере компьютерной информации (ETS № 185) [Электронный ресурс] : заключена в г. Будапеште 23.11.2001 г. — Доступ из СПС «КонсультантПлюс».

6. Копырюлин А.Н. Преступления в сфере компьютерной информации: уголовно-правовой и криминологический аспекты : автореф. дис. ... канд. юрид. наук : 12.00.08 / А.Н. Копырюлин. — Тамбов, 2007. — 22 с.

7. Криминология : учебник / под общ. ред. А.И. Долговой. — 4-е изд., перераб. и доп. — М. : Норма : ИНФРА-М, 2013. — 1008 с.

8. Номоконов В.А. Киберпреступность как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропина // Криминология: вчера, сегодня, завтра. — 2012. — № 24. — С. 45–55.

9. О направлении статистических сведений : письмо ФКУ «ГИАЦ МВД России» от 05.03.2014 г., исх. № 34/4 — 158.

10. Сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации [Электронный ресурс] : свод. сб. по России за янв. — дек. 2010 г. (Ф-615 кн. 1). — Режим доступа: http://giz.mvd.ru.

11. Сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации [Электронный ресурс] : свод. сб. по России за янв. — дек. 2011 г. (Ф-615 кн. 1). — Режим доступа: http://giz.mvd.ru.

12. Сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации [Электронный ресурс] : свод. сб. по России за янв. — дек. 2012 г. (Ф-615 кн. 1). — Режим доступа: http://giz.mvd.ru.

13. Собрание законодательства Российской Федерации. — 2013. — № 3. — Ст. 178.

14. Сухаренко А. Киберугроза для кошелька / А. Сухаренко // ЭЖ-Юрист. — 2014. — № 6. — С. 1–3.

15. Чекунов И.Г. Киберпреступность: понятие и классификация / И.Г. Чекунов // Российский следователь. — 2012. — № 2. — С. 37–44.

16. Kaspersky Security Bulletin 2012: Основная статистика за 2012 год [Электронный ресурс]. — Режим доступа: http://www.securelist.com/ru/analysis/208050778/Kaspersky_Security_Bulletin_2012_Osnovnaya_statistika_za_2012_god#6.

17. Broadhurst R. Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime [Electronic resource] / Roderic Broadhurst, Peter Grabosky, Mamoun Alazab, Steve Chon // International Journal of Cyber Criminology. — 2014. — Jan. — June. — Vol. 8, iss. 1. — Mode of access: http://www.cybercrimejournal.com/#aj.

18. ITU Toolkit For Cybercrime Legislation. — ITU, 2009.

19. O'Connell M. Cyber Security without Cyber War / M. O'Connell // Journal of Conflict & Security Law. — 2012. — Vol. 17. — P. 187–209.

20. Smith R.G. Cyber Criminals on Trial / Russell G. Smith, Peter Grabosky, Gregor Urbas // International Journal of Law and Information Technology. — 2012. — Vol. 20. — P. 242–245.

21. Yar M. The Novelty of «Cybercrime»: An Assessment in Light of Routine Activity Theory / M. Yar // European Journal of Criminology. — 2005. — Oct. — Vol. 2. — P. 407–427.

22. Режим доступа: http://digit.ru/business/20130910/405335397.html#ixzz2r1xUjpbf.

23. Режим доступа: http://digit.ru/internet/20130902/405019726.html#ixzz2r20AikwZ.

24. Режим доступа: http://go.symantec.com/norton-report-2013.

25. Режим доступа: http://ria.ru/incidents/20130117/918552526.html.

26. Режим доступа: http://ria.ru/science/20100926/279475025.html.

27. Режим доступа: http://soft.mail.ru/pressrl_page.php?id=46410.

28. Режим доступа: http://translate.yandex.net/tr-url/en-ru.ru/en.wikipedia.org/wiki/CNet_News.

29. Режим доступа: http://www.garant.ru/news/488680.

30. Режим доступа: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=2&.

31. Режим доступа: http://www.securelist.com/ru/analysis/208050777/Kaspersky_Security_Bulletin_2012_Razvitie_ugroz_v_2012_godu.

32. Режим доступа: http://www.securelist.com/ru/analysis/208050779/Kaspersky_Security_Bulletin_2012_Kiberoruzhie.

33. Режим доступа: http://www.securelist.com/ru/blog/207764382/Operatsiya_Red_October_obshirnaya_set_kibershpionazha_protiv_diplomaticheskikh_i_gosudarstvennykh_struktur.

REFERENCES

1. Bessonov V.A. *Viktimologicheskie aspekty preduprezhdeniya prestuplenii v sfere komp'yuternoi informatsii. Kand. Diss.* [Victimological aspects of Cybercrime prevention. Cand. Diss.]. Nizhnii Novgorod, 2000. 249 p.

2. Vekhov V.B., Smagorinskii B.P. (ed.). *Komp'yuternye prestupleniya: sposoby sovershen'iya i raskrytiya* [Cybercrime: commission and investigation]. Moscow, Pravo i zakon Publ., 1996. 182 p.

3. Gulbin Yu. *Cybercrime*. *Rossiiskaya yustitsiya = Russian Justice*, 1997, no. 10, pp. 24–25. (In Russian).

4. Zinina U.V. *Prestupleniya v sfere komp'yuternoi informatsii v rossiiskom i zarubezhnom ugolovnom prave. Avtoref. Kand. Diss.* [Cybercrime in Russian and foreign Criminal Law. Cand. Diss. Thesis]. Moscow, 2007. 33 p.

5. *Convention on Cybercrime (ETS № 185): Budapest, 23.XI.2001.* (In Russian).

6. Kopyryulin A.N. *Prestupleniya v sfere komp'yuternoi informatsii: ugolovno-pravovoi i kriminologicheskii aspekty. Avtoref. Kand. Diss.* [Cybercrime: criminal legal and criminological aspects. Cand. Diss. Thesis]. Tambov, 2007. 22 p.

7. Dolgova A.I. (ed.). *Kriminologiya* [Criminology]. 4th ed. Moscow, Norma Publ., INFRA-M Publ., 2013. 1008 p.

8. Nomokonov V.A., Tropina T.L. Cybercrime as a new criminal threat. *Kriminologiya: vchera, segodnya, zavtra = Criminology: yesterday, today, tomorrow*, 2012, no. 24, pp. 45–55. (In Russian).

9. Ministry of Internal Affairs of the Russian Federation Main Information and Analysis Center Message on statistical data direction dated 05.03.2014, outgoing letter. № 34/4 — 158. (In Russian).

10. Information on Telecommunication crimes and cybercrimes: Jan. — Dec. 2010 Russia information collection. (F-615 book 1). Available at: http://giz.mvd.ru. (In Russian).

11. Information on Telecommunication crimes and cybercrimes: Jan. — Dec. 2011 Russia information collection. (F-615 book 1). Available at: http://giz.mvd.ru. (In Russian).

12. Information on Telecommunication crimes and cybercrimes: Jan. — Dec. 2012 Russia information collection. (F-615 book 1). Available at: http://giz.mvd.ru. (In Russian).

13. *Sobranie zakonodatel'stva Rossiiskoi Federatsii = Legislation Bulletin of the Russian Federation*, 2013, no. 3, Art. 178.

14. Sukharenko A. Cyber threat for the wallet. *EZh-Yurist = EJ-Jurist*, 2014, no. 6, pp. 1–3. (In Russian).

15. Chekunov I.G. Cybercrimes: definition and classification. *Rossiiskii sledovatel' = Russian Investigator*, 2012, no. 2, pp. 37–44. (In Russian).

16. Kaspersky Security Bulletin 2012: 2012 general statistics. Available at: http://www.securelist.com/ru/analysis/208050778/Kaspersky_Security_Bulletin_2012_Osnovnaya_statistika_za_2012_god#6.

17. 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, Jan. — June, vol. 8, iss. 1. Available at: http://www.cybercrimejournal.com/#aj.

18. ITU Toolkit For Cybercrime Legislation. ITU, 2009.

19. O'Connell M. Cyber Security without Cyber War. *Journal of Conflict & Security Law*, 2012, vol. 17, pp. 187–209.

20. Smith R.G., Grabosky P., Urbas G. Cyber Criminals on Trial. *International Journal of Law and Information Technology*, 2012, vol. 20, pp. 242–245.

21. Yar M. The Novelty of «Cybercrime»: An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, 2005, Oct., vol. 2, pp. 407–427.

22. Available at: http://digit.ru/business/20130910/405335397.html#ixzz2r1xUjpbf.

23. Available at: http://digit.ru/internet/20130902/405019726.html#ixzz2r20AikwZ.

24. Available at: http://go.symantec.com/norton-report-2013.

25. Available at: http://ria.ru/incidents/20130117/918552526.html.

26. Available at: http://ria.ru/science/20100926/279475025.html.

27. Available at: http://soft.mail.ru/pressrl_page.php?id=46410.

28. Available at: http://translate.yandex.net/tr-url/en-ru.ru/en.wikipedia.org/wiki/CNet_News.

29. Available at: http://www.garant.ru/news/488680.

30. Available at: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=2&.

31. Available at: http://www.securelist.com/ru/analysis/208050777/Kaspersky_Security_Bulletin_2012_Razvitie_ugroz_v_2012_godu.

32. Available at: http://www.securelist.com/ru/analysis/208050779/Kaspersky_Security_Bulletin_2012_Kiberoruzhie.

33. Available at: http://www.securelist.com/ru/blog/207764382/Operatsiya_Red_October_obshirnaya_set_kibershpionazha_protiv_diplomaticheskikh_i_gosudarstvennykh_struktur.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Липинский Дмитрий Анатольевич — заместитель ректора — директор Института права Тольяттинского государственного университета, доктор юридических наук, профессор, г. Тольятти, Российская Федерация; e-mail: Dmitri8@yandex.ru.

Евдокимов Константин Николаевич — доцент кафедры государственно-правовых дисциплин Иркутского юридического института (филиала) Академии Генеральной прокуратуры РФ, кандидат юридических наук, доцент, г. Иркутск, Российская Федерация; e-mail: kons-evdokimov@yandex.ru.

БИБЛИОГРАФИЧЕСКОЕ ОПИСАНИЕ СТАТЬИ

Липинский Д.А. Политические причины как современные факторы эволюции компьютерной преступности в Российской Федерации / Д.А. Липинский, К.Н. Евдокимов // Криминологический журнал Байкальского государственного университета экономики и права. — 2015. — Т. 9, № 1. — С. 101–110. — DOI: 10.17150/1996-7756.2015.9(1).101-110.

INFORMATION ABOUT AUTHORS

Lipinsky, Dmitry A. — Deputy Rector, Director of the Law Institute of the Togliatti State University, Doctor of Law, Full Professor, Togliatti, Russian Federation; e-mail: Dmitri8@yandex.ru.

Evdokimov, Konstantin N. — Associate Professor of the Chair of State and Law Disciplines of the Irkutsk Law Institute Affiliated with the Academy of the General Prosecutor's Office of the Russian Federation, PhD in Law, Associate Professor, Irkutsk, Russian Federation; e-mail: kons-evdokimov@yandex.ru.

REFERENCE TO ARTICLE

Lipinsky D.A., Evdokimov K.N. Political reasons as modern factors of the evolution of computer crimes in the Russian Federation. *Criminology Journal of Baikal National University of Economics and Law*, 2015, vol. 9, no. 1, pp. 101–110. DOI: 10.17150/1996-7756.2015.9(1).101-110. (In Russian).