УДК 343.9
DOI 10.17150/1996-7756.2016.10(2).322-330

СОВРЕМЕННЫЕ ПОДХОДЫ К ОПРЕДЕЛЕНИЮ ПОНЯТИЯ, СТРУКТУРЫ И СУЩНОСТИ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

С.В. Скляров[1], К.Н. Евдокимов[2]
[1] Академия Генеральной прокуратуры Российской Федерации, г. Москва, Российская Федерация
[2] Иркутский юридический институт (филиал) Академии Генеральной прокуратуры Российской Федерации, г. Иркутск, Российская Федерация

Информация о статье
Дата поступления
14 ноября 2014 г.

Дата принятия в печать
23 марта 2016 г.

Дата онлайн-размещения
29 июня 2016 г.

Ключевые слова
Компьютерная преступность; киберпреступность; интернет-преступность; преступления в сфере компьютерной информации; компьютерные преступления

Аннотация. Актуальность данного научного исследования обусловлена тем, что компьютерная преступность наносит колоссальный вред общественным отношениям в политической, социально-экономической и информационной сферах Российской Федерации, причиняя огромный материальный ущерб.
Целью научной статьи является анализ современных научных подходов к определению понятия, структуры и сущности компьютерной преступности в России.
По мнению авторов, понятие «компьютерная преступность» следует рассматривать в узком и широком смысле.
В узком смысле компьютерная преступность представляет собой совокупность преступлений, при совершении которых в качестве непосредственного объекта выступают охраняемые законом общественные отношения в сфере безопасного создания, хранения, обработки и передачи компьютерной информации, а предметом являются компьютерная информация, средства ее хранения, обработки, передачи и защиты, информационно-телекоммуникационные сети.
Компьютерная преступность в широком смысле — это совокупность преступлений, при совершении которых объектом выступают любые общественные отношения в сфере информационных технологий и безопасного функционирования компьютерной информации. При этом компьютерная информация, средства ее создания, хранения, обработки и передачи, информационно-телекоммуникационные сети не только являются предметом преступного деяния, но и используются в качестве средства и орудия совершения преступления.
Таким образом, компьютерная преступность в широком смысле соотносится с понятиями «киберпреступность», «интернет-преступность», «преступность в сфере компьютерной информации» как целое и часть, поглощая их по смыслу и содержанию, выступая для них более общим понятием.
Структура компьютерной преступности в Российской Федерации включает не только преступления в сфере компьютерной информации, но и большое количество преступных деяний, совершенных с помощью компьютерных и телекоммуникационных технологий, в том числе посредством информационно-телекоммуникационной сети Интернет. При этом в последнее десятилетие российская компьютерная преступность значительно трансформировалась, приобретя высоколатентный, организованный, «профессиональный», трансграничный, транснациональный, политический и экономически направленный характер.

MODERN APPROACHES TO THE CONCEPT, STRUCTURE AND NATURE OF COMPUTER CRIME IN THE RUSSIAN FEDERATION

Sergey V. Sklyarov[1], Konstantin N. Evdokimov[2]
[1] Academy of the General Prosecutor's Office of the Russian Federation, Moscow, the Russian Federation
[2] Irkutsk Law Institute of the Academy of the General Prosecutor's Office of the Russian Federation, Irkutsk, the Russian Federation

Article info
Received
2014 November 14

Abstract. The relevance of this research is determined by the fact that computer crimes are detrimental to the political, economic, social and information relations in the Russian Federation, causing enormous material damage.

ISSN 1996-7756

Accepted
2016 March 23

Available online
2016 June 29

Keywords
Computer crime; cybercrime; internet crime; crimes in the sphere of computer information; computer crimes

The purpose of this paper is the analysis of modern scientific approaches to the definition of the concept, structure and nature of computer crime in Russia.
According to the authors, the concept of «cybercrime» can be understood in the narrow and in the broad sense.
In the narrow sense computer crimes are those whose immediate target is law-protected public relations in the sphere of safe creation, storing, processing and transfer of computer information, and whose object is computer information, means of its storing, processing, transfer and protection, information-telecommunication networks.
Computer crimes in the broad sense are all those crimes whose targets are any public relations in the sphere of information technologies and safe functioning of computer information. In this case computer information and means of its creation, storing, processing and transfer, information-telecommunication networks are not the objects of crime, but are used as means and instruments of committing a crime.
Thus computer crime in the broad sense correlates with the concepts of «cybercrime», «internet crime», «crimes in the sphere of computer information» as the whole and its parts, taking up their meaning and content and acting as a more general term.
The structure of computer crimes in the Russian Federation includes not only crimes in the sphere of computer information, but also a large number of criminal acts committed with the aid of computer and telecommunication technologies, including the information-telecommunication network the Internet. Besides, in the last decade Russian computer crimes have transformed a lot and become highly latent, organized, «professional», trans-border, trans-national, politically and economically-oriented.

Одна из социальных проблем современного технократического общества — появление компьютерной преступности, причиняющей колоссальный вред общественным отношениям в информационной сфере. Ее возникновение стало возможным из-за того, что граждане, используя компьютерные устройства в личных, производственных или служебных целях, имеют слабое представление о программировании и возможностях программного обеспечения, особенностях функционирования средств создания, хранения, обработки, передачи, защиты компьютерной информации, тем самым становясь потенциальными жертвами компьютерных преступников. Поэтому все большую актуальность приобретает вопрос информационной безопасности физических и юридических лиц, т.е. их защиты от несанкционированного доступа к компьютерной информации, вредоносных компьютерных программ и иных компьютерных угроз.

На простой, казалось бы, вопрос, что следует понимать под компьютерной преступностью, в научном сообществе нет однозначного ответа, и до сих пор ведутся многочисленные дискуссии о содержании и значении данного юридического понятия [1–8].

Одни авторы полагают, что компьютерная преступность — это совокупность преступлений, при совершении которых предметом преступных посягательств выступает компьютерная информация, и отождествляют при этом понятия компьютерного преступления и преступления в сфере компьютерной информации [9, с. 9; 10, с. 830].

Т.М. Лопатина считает, что под компьютерной преступностью следует понимать совокупность совершенных на определенной территории за конкретный период преступлений (лиц, их совершивших), непосредственно посягающих на отношения по сбору, обработке, накоплению, хранению, поиску и распространению компьютерной информации, а также преступлений, совершенных с использованием компьютера в целях извлечения материальной выгоды или иной личной заинтересованности [11, с. 39].

Д.В. Добровольский определяет компьютерную преступность как совокупность всех преступлений в сфере информационных технологий, а не только общественно опасных деяний, предметом которых является компьютерная информация [12, с. 45–46].

По мнению А.А. Жмыхова, компьютерная преступность — это совокупность преступлений, совершаемых с помощью компьютерной системы или сети, в рамках компьютерной системы или сети и против компьютерной системы или сети. Таким образом, он относит к компьютерным преступлениям не только преступления в сфере компьютерной информации, но и преступления, связанные с компьютерами, т.е. такие традиционные по характеру преступные деяния, совершенные с помощью вычислительной

ISSN 1996-7756

техники, как кража, мошенничество, причинение вреда и др. [13, с. 18–19].

В ряде научных работ встречается упоминание о киберпреступности — юридическом понятии, которое часто употребляется в научном обороте за рубежом и наиболее полно, по мнению авторов данных работ, отражает преступные деяния в сфере компьютерной информации, а также преступления, совершенные с помощью компьютерных устройств, информационно-телекоммуникационных сетей и информационных технологий [14; 15]. Такой подход предполагает, что компьютерная преступность является только частью киберпреступности как более широкого понятия.

Отдельные ученые в своих работах отождествляют понятия преступности в Интернете, киберпреступности, компьютерной преступности [16, с. 251–253].

Еще один подход предполагает параллельное существование понятий интернет-преступности и компьютерной преступности как части и целого. По мнению, например, Р.И. Дремлюги, не каждое преступление в сфере компьютерной информации представляет собой интернет-преступление, в то же время такие традиционные преступления, как мошенничество, кража, вымогательство и др., совершенные посредством сети Интернет, — это интернет-преступления. Причем их последствия не обязательно должны наступать в сети Интернет [17, с. 44–45].

С учетом описанных выше подходов к пониманию компьютерной преступности полагаем целесообразным рассматривать данное понятие в узком и широком смысле.

В узком смысле, по мнению авторов, компьютерная преступность представляет собой совокупность преступлений, при совершении которых в качестве основного объекта выступают охраняемые законом общественные отношения в сфере безопасного создания, хранения, обработки и передачи компьютерной информации, а предметом являются компьютерная информация, средства ее хранения, обработки, передачи и защиты, информационно-телекоммуникационные сети.

Компьютерная преступность в широком смысле — это совокупность преступлений, при совершении которых объектом выступают любые общественные отношения в сфере информационных технологий и безопасного функционирования компьютерной информации. При этом компьютерная информация, средства ее создания, хранения, обработки и передачи (компьютеры, смартфоны, кассовые аппараты, банкоматы, платежные терминалы и иные компьютерные устройства), информационно-телекоммуникационные сети не только являются предметом преступного деяния, но и используются в качестве средства и орудия совершения преступления.

Таким образом, понятие компьютерной преступности в узком смысле охватывает преступления в сфере компьютерной информации, уголовная ответственность за которые предусмотрена в гл. 28 Уголовного кодекса Российской Федерации, а в широком смысле включает в себя понятия киберпреступности, интернет-преступности, преступности в сфере компьютерной информации, преступности в сфере информационных технологий. Представляется, что такой подход к пониманию компьютерной преступности позволит оценить всю сложность, многообразие, разноуровневость рассматриваемого криминального явления и найти определенный баланс среди существующих научных позиций.

Анализ структуры компьютерной преступности, с точки зрения авторов, следует проводить исходя именно из широкого смысла данного понятия с учетом существующих нормативных, экспертных и доктринальных аспектов.

Например, исследуя «нормативный» подход к структуре компьютерной преступности, в Доктрине информационной безопасности Российской Федерации можно выделить следующие противоправные деяния, выступающие угрозами безопасности информационных и телекоммуникационных средств и систем: противоправные сбор и использование информации; нарушение технологии обработки информации; внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия; разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации; уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи; уничтожение, повреждение, разрушение или хищение машинных и

ISSN 1996-7756

других носителей информации; несанкционированный доступ к информации, находящейся в банках и базах данных, а также иные деяния[1].

В свою очередь, заключенная в Будапеште 23 ноября 2001 г. и ратифицированная почти 50 государствами Конвенция Совета Европы о преступности в сфере компьютерной информации закрепляет пять групп компьютерных преступлений, образующих компьютерную преступность: преступления против конфиденциальности, целостности и доступности компьютерных данных и систем; правонарушения, связанные с использованием компьютерных средств; правонарушения, связанные с содержанием компьютерных данных; правонарушения, связанные с нарушением авторского права и смежных прав; акты расизма и ксенофобии, совершенные посредством компьютерных сетей[2].

Российская Федерация в силу различных политических, юридических, информационных и иных объективных причин не ратифицировала вышеуказанную конвенцию Совета Европы. Однако, несмотря на данный факт, МВД России, к чьей компетенции относится выявление, расследование и раскрытие компьютерных преступлений, придерживается практически аналогичной классификации преступных деяний[3].

В поддержку данной позиции говорит и то, что российский законодатель в ряде статей УК РФ (например, в ст. 171.2, 228.1, 242, 242.1, 242.2) предусмотрел специальный квалифицирующий признак — совершение преступления с использованием средств массовой информации, в том числе информационно-телекоммуникационных сетей (включая сеть Интернет).

Несмотря на сложившийся «нормативный» подход правоохранительных органов к структуре компьютерной преступности, или, как принято говорить в экспертном сообществе, к «рынку киберпреступности», специалисты и эксперты в сфере информационной безопасности имеют собственную точку зрения на структуру компьютерной преступности в Российской Федерации.

В частности, эксперты международной компании Group-IB, специализирующейся на предупреждении и расследовании киберпреступлений, считают, что основными преступными деяниями, образующими «рынок киберпреступности» в России, являются:

– мошенничество в системах интернет-банкинга;
– фишинг;
– хищение электронных денег;
– услуги обналичивания иных нелегальных доходов;
– спам (противоправная реклама медикаментов и различной контрафактной продукции, поддельного программного обеспечения, незаконное распространение информации об услугах в сферах обслуживания, образования, туризма и др.);
– продажа трафика;
– продажа эксплойтов;
– продажа загрузок;
– анонимизация;
– DDoS-атаки[4].

В свою очередь, специалисты Центра глобальных исследований и анализа угроз «Лаборатории Касперского» (GReAT), анализирующие ежегодное состояние киберпреступности в России и других странах мира, к компьютерным преступлениям (на профессиональном сленге — к компьютерным угрозам), составляющим киберпреступность, относят:

– целевые кибератаки;
– кибершпионаж;
– хактивизм;
– кражу конфиденциальных данных;
– кибервымогательство;
– кибератаки, совершаемые по найму (кибернаемничество);
– использование вредоносного программного обеспечения для мобильных устройств;
– целевой фишинг;
– нарушение тайны частной жизни;
– использование эксплойтов для уязвимостей программного обеспечения;
– кибервымогательство;
– создание и использование ботнетов[5].

[1] Доктрина информационной безопасности Российской Федерации : утв. Президентом РФ 9 сент. 2000 г. № Пр-1895 // Российская газета. 2000. 28 сент.

[2] Конвенция о преступности в сфере компьютерной информации (ETS N 185) : заключена в Будапеште 23 нояб. 2001 г. // Собрание законодательства Российской Федерации. 2005. № 47. Ст. 4929.

[3] Сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации [Электронный ресурс] : свод. сб. по России (Ф. 615 КН. 1). URL : http://mvd.ru.

[4] Group-IB [Электронный ресурс] : офиц. сайт. URL : http://report2013.group-ib.ru.

[5] URL : http://securelist.ru/files/2014/12/Kaspersky-Security-Bulletin-2014-RU.pdf.

ISSN 1996-7756

По мнению экспертов лаборатории PandaLabs, входящей в состав международной компании Panda, производящей антивирусное программное обеспечение, в 2015 г. основными преступными деяниями, формирующими компьютерную преступность в России, стали:

– кибершантаж (например, вредоносные программы типа CryptoLocker, которые после проникновения в компьютер шифруют все типы документов, могущих представлять ценность для пользователя (электронные таблицы, документы, базы данных, фотографии и пр.), после чего киберпреступники начинают шантажировать свою жертву, требуя заплатить выкуп за возможность восстановления файлов);

– направленные кибератаки на информационные ресурсы компаний, организаций, учреждений и т.д.;

– кибератаки на платежные терминалы для кражи данных банковских карт клиентов;

– APT-атаки (APT — Advanced Persistent Threats) — так называемые постоянные угрозы повышенной сложности, представляющие собой вид направленных атак, которые нацелены на крупные компании или стратегически важные институты;

– взлом подключенных к Интернету устройств («интернет-вещей»), от IP-камер и до принтеров, которые, являясь частью Интернета, обладают программным обеспечением, что делает их весьма уязвимыми для взлома киберпреступниками и причинения ущерба пользователю;

– атаки на смартфоны, а также иные мобильные устройства с целью кражи паролей и данных пользователей[6].

Таким образом, мнение экспертного сообщества о структуре компьютерной преступности и компьютерных преступлениях несколько отличается от «нормативного» подхода правоохранительных органов, так как основывается на программно-технических критериях, однако не противоречит ему, поскольку практически все так называемые киберугрозы подпадают под действие УК РФ.

Исследование научной литературы по рассматриваемой теме также показывает неоднозначность мнений ученых относительно структуры компьютерной преступности в России.

Например, Д.К. Чирков и А.Ж. Саркисян в структуре компьютерной преступности выделяют только те преступные деяния, которые учитываются ГИАЦ МВД России как преступления, совершенные в сфере телекоммуникаций и компьютерной информации [18, с. 220].

По мнению М.Б. Эмирова, А.Д. Саидова, Д.А. Рагимханова, к наиболее распространенным видам преступлений в глобальных компьютерных сетях можно отнести промышленный шпионаж, саботаж, вандализм, спуфинг (взлом паролей), мошенничество [19, с. 65].

Другие авторы исходят из сложной структуры компьютерной преступности и рассматривают входящие в нее преступные деяния по нескольким критериям: объект, предмет посягательства, способ совершения и т.п. [11, с. 34–37; 20, с. 48]. Например, по объекту посягательства выделяются следующие группы компьютерных преступлений: преступления против конфиденциальности, целостности, доступности компьютерных данных и компьютерных сетей; экономические компьютерные преступления; компьютерные преступления против личных прав и неприкосновенности частной сферы; компьютерные преступления против общественных и государственных интересов [21, с. 150].

По мнению авторов, для оценки структуры компьютерной преступности в России предпочтительней использовать классификацию и статистику совершенных компьютерных преступлений, применяемые правоохранительными органами, т.е. «нормативный» подход. Это обусловлено тем, что существующая методика учета зарегистрированных, расследованных, приостановленных и прекращенных уголовных дел по преступлениям данного вида уже апробирована временем, а уголовная статистика складывается из ежедневно поступающих данных от территориальных органов ФСБ, МВД, Следственного комитета Российской Федерации. В силу этого правоохранительные органы обладают бóльшим объемом аналитической информации о структуре и масштабах компьютерной преступности в России, чем экспертное или научное сообщество, что не умаляет роли последних в исследовании данного криминального явления.

Так, на основании статистических данных ГИАЦ МВД России можно утверждать, что примерная структура российской компьютерной преступности выглядит следующим образом:

[6] URL : http://www.viruslab.ru/upload/files/download/wp/wp_reports_2014.pdf.

ISSN 1996-7756

– нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан (ч. 1 ст. 138 УК РФ) — 0,40 %;

– незаконный оборот специальных технических средств, предназначенных для негласного получения информации (ст. 138.1 УК РФ), — 2,40 %;

– неправомерный доступ к компьютерной информации (ст. 272 УК РФ) — 21,20 %;

– создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) — 9,80 %;

– нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) — 0,02 %;

– нарушение авторских и смежных прав, совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 146 УК РФ), — 11,10 %;

– кража, совершенная с использованием компьютерных и телекоммуникационных технологий (ст. 158 УК РФ), — 9,78 %;

– мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) и мошенничество, совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 159 УК РФ), — 30,20 %;

– причинение имущественного ущерба путем обмана или злоупотребления доверием, совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 165 УК РФ), — 0,20 %;

– незаконные организация и проведение азартных игр, совершенные с использованием компьютерных и телекоммуникационных технологий (ст. 171.2 УК РФ), — 0,20 %;

– незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, совершенные с использованием компьютерных и телекоммуникационных технологий (ст. 183 УК РФ), — 2,80 %;

– незаконные изготовление и оборот порнографических материалов или предметов, совершенные с использованием компьютерных и телекоммуникационных технологий (ст. 242 УК РФ), — 6,10 %;

– изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних, совершенные с использованием компьютерных и телекоммуникационных технологий (ст. 242.1 УК РФ), — 5,30 %;

– использование несовершеннолетнего в целях изготовления порнографических материалов или предметов, совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 242.2 УК РФ), — 0,50 %[7].

Как видно, среди преступных деяний, образующих компьютерную преступность в Российской Федерации, преобладают: мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) и мошенничество, совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 159 УК РФ), — 30,20 %; неправомерный доступ к компьютерной информации (ст. 272 УК РФ) — 21,20 %; нарушение авторских и смежных прав, совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 146 УК РФ), — 11,10 %; создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) — 9,80 %; кража, совершенная с использованием компьютерных и телекоммуникационных технологий (ст. 158 УК РФ), — 9,78 %.

Таким образом, наибольший удельный вес среди совершенных компьютерных преступлений приходится на мошенничество в сфере компьютерной информации и преступления в сфере компьютерной информации, которые в настоящее время составляют основу компьютерной преступности в России.

Рассуждая о сущности компьютерной преступности в Российской Федерации, можно заключить, что компьютерная преступность:

– является разновидностью российской преступности, существующей наравне с экономической, насильственной, коррупционной, экологической и иными видами преступности;

– тесно взаимосвязана с другими видами преступности в Российской Федерации, поскольку преступления в сфере компьютерной информации часто выступают способом совершения других уголовных деяний (кража, вымогательство, незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, государственная измена, шпионаж и др.);

[7] 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). URL : http://mvd.ru.

ISSN 1996-7756

– носит высокотехнологичный характер, что вызвано использованием IT-технологий, информационно-телекоммуникационных сетей, компьютерных устройств, носителей компьютерной информации и т.п., которые выступают орудиями и средствами совершения компьютерных преступлений;

– обладает высокой степенью латентности, которая составляет от нескольких десятков до нескольких тысяч процентов по разным видам преступных деяний, что обусловлено различными объективными факторами (нежелание жертв компьютерных преступлений обращаться в правоохранительные органы, незаметность компьютерных преступлений для большинства населения в силу их совершения в виртуальной среде, сложность выявления компьютерных преступлений при отсутствии необходимого количества специалистов в правоохранительных структурах и т.д.);

– носит высокоорганизованный характер и тесно связана с организованной преступностью, так как значительное количество компьютерных преступлений (DDoS-атаки, банкинг, фишинг, создание ботнетов и др.) совершается организованными преступными группами;

– имеет «профессиональный» характер, так как лица, совершающие компьютерные преступления, обладают преступной специализацией, не совершая иных видов преступных деяний; получают преступный доход (прибыль) в результате преступной деятельности; имеют необходимые знания, умения, навыки в сфере IT-технологий для совершения преступления; придерживаются определенных правил, законов, понятий и терминологии, позволяющих им общаться, обмениваться опытом и находить единомышленников;

– характеризуется трансграничностью, так как киберпространство существует вне государственных границ и, будучи общедоступным, позволяет преступнику, находящемуся на территории одного государства, совершать преступления в отношении лиц, находящихся в другом государстве;

– носит транснациональный характер, так как компьютерные преступники в силу своей принадлежности к компьютерному «андеграунду» для получения преступных доходов, облегчения совершения преступных деяний на территории двух и более государств вынуждены, независимо от национальности, объединяться в международные преступные группы;

– находится в состоянии динамического развития, что обусловлено постоянным совершенствованием существующих и созданием новых IT-технологий, вовлечением в информационные отношения новых участников, расширением киберпространства за счет увеличения числа пользователей сети Интернет, мобильных компьютерных устройств, переходом к электронному документообороту все большего количества организаций, предприятий, учреждений;

– обрела черты экономической преступности, так как большинство компьютерных преступлений совершается в банковско-финансовом или корпоративном секторе (интернет-банкинг, банковский фишинг, кибервымогательство и т.д.), а деятельность преступников направлена на извлечение доходов (прибыли);

– трансформируется в преступность политического характера, что связано с активизацией противоправной деятельности в киберпространстве Российской Федерации представителей хактивистского движения, спецслужб и силовых структур зарубежных государств, международных экстремистских и террористических организаций (DDoS-атаки на правительственные сайты, кибершпионаж в отношении информационных ресурсов органов государственной власти, силовых ведомств, предприятий оборонно-промышленного комплекса, дипломатических представительств, распространение в сети Интернет экстремистских материалов, вербовка новых членов в террористические организации и т.д.).

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Евдокимов К.Н. Политические факторы компьютерной преступности в России / К.Н. Евдокимов // Информационное право. — 2015. — № 1. — С. 41–47.

2. Ефремова М.А. Уголовная ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий / М.А. Ефремова. — М. : Юрлитинформ, 2015. — 200 с.

3. Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ / И.Г. Смирнова, К.Н. Евдокимов, О.А. Егерева [и др.] ; под науч. ред. И.Г. Смирновой. — М. : Юрлитинформ, 2016. — 312 с.

4. Степанов-Егиянц В.Г. Проблемы разграничения неправомерного доступа к компьютерной информации со смежными составами / В.Г. Степанов-Егиянц // Право и кибербезопасность. — 2014. — № 2. — С. 27–32.

5. 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.

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

7. 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. — Vol. 8, iss. 1. — Mode of access : http://www.cybercrimejournal.com/#aj.

8. Yar M. The novelty of 'cybercrime': an assessment in light of routine activity theory / M. Yar // European Journal of Criminology. — 2005. — Vol. 2. — P. 407–427.

9. Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации: (по материалам Республики Дагестан) : дис. ... канд. юрид. наук : 12.00.08 / М.С. Гаджиев. — Махачкала, 2004. — 168 с.

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

11. Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности : дис. ... д-ра юрид. наук : 12.00.08 / Т.М. Лопатина. — М., 2007. — 418 с.

12. Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью : дис. … канд. юрид. наук : 12.00.08 / Д.В. Добровольский. — М., 2005. — 218 с.

13. Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение : дис. … канд. юрид. наук : 12.00.08 / А.А. Жмыхов. — М., 2003. — 178 с.

14. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : дис. … канд. юрид. наук : 12.00.08 / Т.Л. Тропина. — Владивосток, 2005. — 235 с.

15. Чекунов И.Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности : автореф. дис. … канд. юрид. наук : 12.00.08 / И.Г. Чекунов. — М., 2013. — 22 с.

16. Рассолов И.М. Право и Интернет. Теоретические проблемы / И.М. Рассолов. — М. : Норма, 2003. — 332 с.

17. Дремлюга Р.И. Интернет-преступность / Р.И. Дремлюга. — Владивосток : Изд-во Дальневост. ун-та, 2008. — 240 с.

18. Чирков Д.К. Преступность в сфере телекоммуникаций и компьютерной информации как угроза национальной безопасности страны / Д.К. Чирков, А.Ж. Саркисян // Актуальные проблемы экономики и права. — 2013. — № 3. — С. 219–226.

19. Эмиров М.Б. Борьба с преступлениями в глобальных компьютерных сетях / М.Б. Эмиров, А.Д. Саидов, Д.А. Рагимханов // Юридический вестник Дагестанского государственного университета. — 2011. — № 2. — С. 63–66.

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

21. Номоконов В.А. Киберпреступность: прогнозы и проблемы борьбы / В.А. Номоконов, Т.Л. Тропина // Библиотека криминалиста. — 2013. — № 5 (10). — С. 148–160.

REFERENCES

1. Evdokimov K.N. Political factors of computer crime in Russia. *Informazionnoe pravo = Information Law*, 2015, no. 1, pp. 41–47. (In Russian).

2. Efremova M.A. *Ugolovnaya otvetstvennost' za prestupleniya*, *sovershaemye s ispol'zovaniem informatsionno-telekommunikatsionnykh tekhnologii* [Criminal liability for crimes committed with the use of information and telecommunication technologies]. Moscow, Yurlitinform Publ., 2015. 200 p.

3. Smirnova I.G., Evdokimov K.N., Egereva O.A. et al. *Kiberprestupnost': kriminologicheskii, ugolovno-pravovoi, ugolovno-protsessual'nyi i kriminalisticheskii analiz* [Cybercrimes: A Criminological, Criminal Law, Criminal Process and Criminalistic Analysis]. Moscow, Yurlitinform Publ., 2016. 312 p.

4. Stepanov-Egiyanz V.G. Problems of delimitation of illegal access to computer information with neighboring elements. *Pravo i kiberbezopasnost' = Law and Cyber Security*, 2014, no. 2, pp. 27–32. (In Russian).

5. Smith Russell G., Grabosky Peter, Urbas Gregor. Cyber criminals on trial. *International Journal of Law and Information Technology*, 2012, vol. 20, pp. 242–245.

6. O'Connell M. Cyber security without cyber war. *Journal of Conflict & Security Law*, 2012, vol. 17, pp.187–209.

7. Broadhurst Roderic, Grabosky Peter, Alazab Mamoun, Chon Steve. Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology*, 2014, vol. 8, iss. 1. Available at: http://www.cybercrimejournal.com/#aj.

8. Yar M. The novelty of 'cybercrime': an assessment in light of routine activity theory. *European Journal of Criminology*, 2005, vol. 2, pp. 407–427.

9. Gadzhiev M.S. *Kriminologicheskii analiz prestupnosti v sfere komp'yuternoi informatsii* (*po materialam Respubliki Dagestan*). *Kand. Diss*. [Criminological Analysis of Crimes in the Sphere of Computer Information (based on the materials of the Republic of Dagestan). Cand. Diss.]. Makhachkala, 2004. 168 p.

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

11. Lopatina T.M. *Kriminologicheskie i ugolovno-pravovye osnovy protivodeistviya komp'yuternoi prestupnosti. Dokt. Diss*. [Criminological and Criminal Law Basis of Counteracting Cybercrimes. Doct. Diss.]. Moscow, 2007. 418 p.

12. Dobrovol'skii D.V. *Aktual'nye problemy bor'by s komp'yuternoi prestupnost'yu. Kand. Diss*. [Topical Issues of Fighting Computer Crimes. Cand. Diss.]. Moscow, 2005. 218 p.

ISSN 1996-7756

13. Zhmyhov A.A. *Komp'yuternaya prestupnost' za rubezhom i ee preduprezhdenie*. *Kand. Diss*. [Computer Crimes in other Countries and their Prevention. Cand. Diss.]. Moscow, 2003. 178 p.

14. Tropina T.L. *Kiberprestupnost': ponyatie, sostoyanie, ugolovno-pravovye mery bor'by. Kand. Diss*. [Cybercrimes: Concept, Condition, Criminal Law Counteraction Measures. Cand. Diss.]. Vladivostok, 2005. 235 p.

15. Chekunov I.G. *Kriminologicheskoe i ugolovno-pravovoe obespechenie preduprezhdeniya kiberprestupnosti. Avtoref. Kand. Diss.* [Criminological and Criminal Law Provisions of Cybercrime Prevention. Diss. Cand. Thesis]. Moscow, 2013. 23 p.

16. Rassolov I.M. *Pravo i Internet: teoreticheskie problemy* [The Law and the Internet. Theoretical Issues]. Moscow, Norma Publ., 2003. 332 p.

17. Dremluga R.I. *Internet-prestupnost'* [Internet Crimes]. Vladivostok, Far-Eastern Federal University Publ., 2008. 240 p.

18. Chirkov D.K., Sarkisyan A.J. Crimes in the sphere of telecommunications and computer information as a threat to the national security of the country. *Aktual'nye problemy ekonomiki i prava = Actual Problems of Economics and Law*, 2013, no. 3, pp. 219–226. (In Russian).

19. Emirov M.B., Saidov A.D., Ragimkhanov D.A. Fighting Crimes in Global Computer Networks. *Yuridicheskii vestnik Dagestanskogo gosudarstvennogo universiteta = Law Bulletin of Dagestan State University*, 2011, no. 2, pp. 63–66. (In Russian).

20. 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).

21. Nomokonov V.A., Tropina T.L. Cybercrime: Forecasts and Problems of Fighting. *Biblioteka kriminalista = Criminalist's Library*, 2013, no. 5 (10), pp. 148–160. (In Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Скляров Сергей Валерьевич — проректор Академии Генеральной прокуратуры Российской Федерации, доктор юридических наук, профессор, г. Москва, Российская Федерация; e-mail: sklyarovsv@mail.ru.

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

БИБЛИОГРАФИЧЕСКОЕ ОПИСАНИЕ СТАТЬИ

Скляров С.В. Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации / С.В. Скляров, К.Н. Евдокимов // Криминологический журнал Байкальского государственного университета экономики и права. — 2016. — Т. 10, № 2. — С. 322–330. — DOI : 10.17150/1996-7756.2016.10(2).322-330.

INFORMATION ABOUT THE AUTHORS

Sklyarov, *Sergey V.* — Provost, the Academy of the General Prosecutor's Office of the Russian Federation, Doctor of Law, Professor, Moscow, the Russian Federation; e-mail: sklyarovsv@mail.ru.

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

BIBLIOGRAPHIC DESCRIPTION

Sklyarov S.V., Evdokimov K.N. Modern approaches to the concept, structure and nature of computer crime in the Russian Federation. *Criminology Journal of Baikal National University of Economics and Law*, 2016, vol. 10, no. 2, pp. 322–330. DOI: 10.17150/1996-7756.2016.10(2).322-330. (In Russian).