УДК 343.98 № 1 (16) / 2018, с. 89—93

ПРОБЛЕМЫ БОРЬБЫ С КИБЕРТЕРРОРИЗМОМ

Виталий Борисович Вехов
Московский государственный технический университет имени Н. Э. Баумана
E-mail: v-vehov@mail.ru

Сергей Александрович Ковалев
Волгоградская академия Министерства внутренних дел Российской Федерации
E-mail: skovalv@mail.ru

В статье исследуются теоретические и прикладные проблемы противодействия преступлениям нового вида, получившего условное название «кибертерроризм». Анализируются действующие международные и отечественные нормативные правовые акты, регулирующие отношения в этой сфере. Формулируются актуальные проблемы, возникающие в деятельности сотрудников органов предварительного расследования по борьбе с ними.

Ключевые слова: кибертерроризм, киберпреступления, информационное оружие, DDoS-атака, информационная война.

PROBLEMS OF FIGHT AGAINST CYBERTERRORISM

V. B. Vekhov

S. A. Kovalev

In article theoretical and applied problems of counteraction to crimes of the new look which has received the conditional name "cyberterrorism" are investigated. The existing international and domestic regulations governing the relations in this sphere are analyzed. The current problems arising in activities of staff of bodies of preliminary investigation for fight against them are formulated.

Keywords: cyberterrorism, cybercrimes, information weapon, DDoS-attack, information war.

Глобальная информатизация мирового сообщества и развитие компьютерной сети Интернет привели к тому, что информационно-телекоммуникационные инфраструктуры промышленно развитых стран оказались весьма уязвимыми объектами воздействия со стороны террористических организаций. Угрозы международного кибертерроризма и информационных войн стали, во-первых, объективной реальностью XXI века, во-вторых, важными геополитическими факторами, определяющими векторы развития человеческой цивилизации. Так, в опубликованном Руководстве по предотвращению и контролю над преступлениями, связанными с использованием сети Интернет, для стран — членов ООН эти преступные посягательства названы глобальной международной проблемой [1]. Аналогичные по смыслу положения содержатся и в других международных правовых актах: Конвенции Совета Европы о киберпреступности [2], Окинавской Хартии глобального информационного общества [3], Бангкокской декларации о противодействии новым видам киберпреступлений [4].

В новой Доктрине информационной безопасности Российской Федерации (2016 года) подчеркивается, что возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военнополитических, а также террористических целей в ущер международной безопасности и стратегической стабильности [5, п. 10].

В настоящее время различные террористические организации широко используют механизмы информационного воздействия

на индивидуальное, групповое и общественное сознание для нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, а также для привлечения к террористической деятельности новых сторонников. В противоправных целях ими активно создаются и (или) добываются (приискиваются) различными способами высокотехнологические программно-технические средства деструктивного воздействия на объекты критической информационной инфраструктуры [5, п. 13].

По этому поводу следует заметить, что в отличие от обычного террориста, применяющего для совершения преступного деяния традиционные виды оружия и взрывных устройств, киберпреступник использует для реализации поставленных целей такую разновидность информационного оружия, как специальные программно-технические средства, предназначенные (разработанные, приспособленные, запрограммированные) для негласного получения, изменения, уничтожения или блокирования информации, содержащейся на электронных носителях, в ЭВМ и других компьютерных устройствах, информационных системах или компьютерных сетях.

В связи с чем, состояние информационной безопасности характеризуется постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных террористических атак, а также нарастанием угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической, социальной и финансовой стабильности нашего государства [5, п. 16].

Известно, что за последние 5 лет в России в числе выявленных тяжких и особо тяжких преступлений, вызвавших повышенный общественный резонанс, широкое распространение получили преступные посягательства террористической направленности, совершенные с использованием информационно-телекоммуникационных сетей, их сервисов, в том числе так называемых «социальных сетей», вредоносных компьютерных программ и управляемых с их помощью скрытно для других пользователей компьютерных сетей — так называемых «ботнетов» (образовано от англ. слов «robot» — робот и «network» — сеть).

К сожалению, существующее в настоящее время распределение между странами ресурсов, необходимых для обеспечения безопасного и устойчивого функционирования сети Интернет, не позволяет реализовать совместное справедливое, основанное на принципах доверия управление ими. Отсутствие международных правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационно-телекоммуникационных технологий, затрудняет формирование системы международной информационной безопасности от актов кибертерроризма [5, п. 19].

В связи с чем, массовый характер приобрели сетевые распределенные атаки на WEB-серверы коммерческих структур, кредитно-финансовых организаций, органов государственной законодательной, судебной и исполнительной власти, включая силовые ведомства и правоохранительные органы. Речь идет о так называемых «DDoS-атаках» (от англ. «Distributed Denial of Service» — отказ в обслуживании), об особенностях расследования которых мы писали ранее [6]. О степени их общественной опасности наглядно свидетельствуют следующие данные.

1. В 2015 году ФСБ России было зафиксировано 24 млн атак на официальные сайты и информационные системы органов государственной власти, а также пресечено функционирование более 1,6 тысяч Интернет-ресурсов, деятельность которых наносила ущерб безопасности нашей страны, в том числе террористической направленности [7].

2. В 2016 году на российские объекты критической информационной инфраструктуры было совершено более 70 млн террористических кибератак (примерно, в три раза больше, чем за предыдущий год) [8].

3. В первом полугодии 2017 года Россия заняла второе место по числу кибератак (10 % от всех совершенных в мире, как с территории страны, так и извне). На первом месте находятся США (41 % атак), на третьем — Великобритания (7 % атак) [9].

4. Потери от кибертерроризма во всем мире к 2018 году могут вырасти минимум в четыре раза и достигнуть 2 трлн долл. США [10].

5. Как правило, большинство DDoS-атак являются мультивекторными: для их усложнения используется одновременно несколько способов воздействия на атакуемую информационную систему, тем самым, защититься от них становится значительно труднее и при этом, изменение вектора атаки не требует от кибертеррориста существенных временных затрат [11, с. 17].

Нельзя также не отметить и то обстоятельство, что интенсивно развивающиеся в настоящее время частные электронные платежные системы, обеспечивающие не урегулированный действующим отечественным законодательством оборот виртуальных денег, в том числе криптовалют, способствуют террористической деятельности. По информации из Следственного комитета Российской Федерации транзакции в них производятся анонимно, без централизованного контроля и полулегально, что мотивирует кибертеррористов использовать данные платежно-расчетные инструменты в своей преступной деятельности, например, для оплаты незаконно поставляемых запрещенной в России террористической организацией ИГИЛ нефти и газа, вербовки новых членов. О необходимости запрета подобного рода платежных средств указано и в рекомендациях, подготовленных по итогам экстренной встречи министров юстиции стран ЕС, прошедшей в ноябре 2015 года в Брюсселе (встреча прошла после терактов во Франции) [12].

Для эффективного противодействия рассматриваемым преступным посягательствам в соответствии с Указом Президента Российской Федерации от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации» были осуществлены следующие действенные мероприятия:

1) сегмент международной информационно-телекоммуникационной сети Интернет, используемый органами законодательной, судебной и исполнительной власти, в том числе правоохранительными и субъектов Российской Федерации, находящийся в ведении ФСО России, преобразован в российский государственный сегмент этой сети;

2) утвержден единый порядок подключения информационных систем и информационно-телекоммуникационных сетей к сети Интернет и размещения (публикации) в ней информации через названный сегмент, предусматривающий ее передачу по каналам связи, защищенным с использованием шифровальных (криптографических) средств.

Начиная с 2013 года, ФСБ России создается государственная система обнаружения, предупреждения и ликвидации последствий компьютерных, в том числе террористических атак на информационные ресурсы Российской Федерации — информационные системы и информационно-телекоммуникационные сети, находящиеся на территории России и в наших дипломатических представительствах и консульских учреждениях за рубежом. Система получила условное название «ГосСОПКА» [13; 14]. Основными ее задачами являются [13]:

а) прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации;

б) обеспечение взаимодействия владельцев информационных ресурсов, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак;

в) осуществление контроля степени защищенности критической информационной инфраструктуры России от компьютерных атак;

г) установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации.

Продолжая исследование обозначенной проблематики, отметим, что раскрытие и расследование преступлений выделенного вида остается довольно сложной задачей для большинства сотрудников органов предварительного расследования. Помимо изложенных, это обусловлено следующими объективными и субъективными факторами:

1) отсутствием обобщений материалов следственной и судебной практики;

2) отсутствием методических рекомендаций по организации раскрытия и расследования преступных посягательств кибертеррористической направленности;

3) отсутствием опыта работы у следователей и работников органов дознания со специфическими источниками доказательственной информации, находящейся в виде электронных сообщений и документов, страниц и сайтов сети Интернет;

4) недостаточным уровнем подготовки специалистов соответствующего профиля в высших учебных заведениях, которых в соответствии с действующим уголовно-процессуальным законодательством в обязательном порядке необходимо привлекать для участия в следственных действиях;

5) недоступностью компетентных специалистов в области работы с компьютерной информацией и ее электронными носителями для подавляющего числа сотрудников органов предварительного расследования [15, с. 158].

Особенности механизма совершения рассматриваемых преступных посягательств,

специфичность следовых картин, высокая динамика их развития и изменения, недостаточное правовое урегулирование общественных отношений в данной сфере, противоречивость национального законодательства и соответствующего терминологического аппарата в разных государствах препятствуют эффективной борьбе с преступлениями выделенного вида.

С учетом изложенного видится обоснованным вывод о том, что в современных условиях кибертерроризм представляет собой серьезную угрозу национальной безопасности не только России, но и других стран. На этом основании борьба с ним является приоритетной задачей правоохранительных органов, выполнение которой сопряжено со значительными трудностями.

Список литературы

1. Эффективное предупреждение преступности: в ногу с новейшими достижениями // Материалы Десятого Конгресса Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями : A/CONF.187/10. — Вена, 10-17 апреля 2000 г. — П. 5.

2. Конвенция Совета Европы «О киберпреступности» от 23.11.2001 г. ETS № 185 (Будапешт) [Электронный ресурс] // Официальный сайт Министерства внутренних дел Республики Беларусь. — URL: http://mvd.gov.by/main.aspx?guid=4603 (дата обращения: 16.06.2017).

3. Хартия глобального информационного общества от 23.07.2000 г. (принята на Окинаве (Япония) на совещании руководителей Глав государств и правительств стран «Группы Восьми») // Дипломатический вестн. — 2000. — № 8. — С. 51—56.

4. Меры по борьбе против преступлений, связанных с использованием компьютеров // Материалы Одиннадцатого Конгресса Организации Объединенных Наций по предупреждению преступности и уголовному правосудию : A/CONF.203/14. — Бангкок, 18—25 апреля 2005 г.

5. Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента Российской Федерации от 05.12.2016 № 646 [Электронный ресурс] // Информационно-правовой портал ГАРАНТ.РУ. - URL: http://www.garant.ru/products/ipo/prime/doc/71456224/ (дата обращения: 16.06.2017).

6. Вехов, В. Б. Особенности расследования DDoS-атак, совершенных на web-серверы организаций / В. Б. Вехов // Проблемы борьбы с преступностью: российский и международный опыт : сб. науч. тр. — Волгоград : ВА МВД РФ, 2009. — Вып. 1. — С. 25—34.

7. Путин: ФСБ зафиксировала за год 24 миллиона атак хакеров на сайты госорганов [Электронный ресурс] // ТВ-Центр. — URL: http://www.tvc.ru/news/show/id/87426 (дата обращения: 16.06.2017).

8. ФСБ помогла российским банкам нейтрализовать кибератаки в ноябре 2016 года [Электронный ресурс] // INTERFAX.RU. — URL: http://www.interfax.ru/russia/547287 (дата обращения: 16.06.2017).

9. Россия стала второй после США по количеству кибератак [Электронный ресурс] // SorokaInfo.com. — URL: http://sorokainfo.com/news/rossija_stala_vtoroj_posle_ssha_po_kolichestvu_kiberatak/2017-06-13-3434 (дата обращения: 16.06.2017).

10. Сбербанк: потери от киберугроз в мире к 2018 году могут вырасти в четыре раза [Электронный ресурс] // ТАСС. — URL: http://tass.ru/ekonomika/3355825 (дата обращения: 16.06.2017).

11. Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России за период с 01 июня 2015 года по 31 мая 2016 года [Электронный ресурс] // Центральный Банк Российской Федерации : официальный сайт. — URL: http://www.cbr.ru/credit/Gubzi_docs/fincert_survey.pdf (дата обращения: 16.06.2017).

12. Козлова, Н. Обман валют [Электронный ресурс] / Н. Козлова // Российская газета. — Федеральный выпуск № 6874 (6). — URL: http://rg.ru/2016/01/15/bastrykin.html (дата обращения 16.06.2017).

13. О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации : Указ Президента Российской Федерации от 15.01.2013 № 31с [Электронный ресурс] // Президент России : официальный сайт. — URL: http://www.kremlin.ru/acts/bank/36691 (дата обращения 16.06.2017).

14. Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утв. Президентом Российской Федерации 12.12.2014 № К 1274) [Электронный ресурс] // Федеральная служба безопасности Российской Федерации : официальный сайт. — URL: http://www.fsb.ru/files/PDF/Vipiska_iz_koncepcii.pdf (дата обращения 16.06.2017).

15. Вехов, В. Б. Понятие, виды и особенности фиксации электронных доказательств / В. Б. Вехов // Расследование преступлений: проблемы и пути их решения. — 2016. — № 1. — С. 155—158.

References

1. Ehffektivnoe preduprezhdenie prestupnosti: v nogu s novejshimi dostizheniyami // Materialy Desyatogo Kongressa Organizacii Ob"edinennyh Nacij po preduprezhdeniyu prestupnosti i obrashcheniyu s pravonarushitelyami : A/CONF.187/10. — Vena, 10 17 aprelya 2000 g. — P. 5.

2. Konvenciya Soveta Evropy «O kiberprestupnosti» ot 23.11.2001 g. ETS № 185 (Budapesht) [Ehlektronnyj resurs] // Oficial'nyj sajt Ministerstva vnutrennih del Respubliki Belarus'. — URL: http://mvd.gov.by/main.aspx?guid=4603 (data obrashcheniya: 16.06.2017).

3. Hartiya global'nogo informacionnogo obshchestva ot 23.07.2000 g. (prinyata na Okinave (YAponiya) na soveshchanii rukovoditelej Glav gosudarstv i pravitel'stv stran «Gruppy Vos'mi») // Diplomaticheskij vestn. — 2000. — № 8. — S. 51—56.

4. Mery po bor'be protiv prestuplenij, svyazannyh s ispol'zovaniem komp'yuterov // Materialy Odinnadcatogo Kongressa Organizacii Ob"edinennyh Nacij po preduprezhdeniyu prestupnosti i ugolovnomu pravosudiyu : A/CONF.203/14. — Bangkok, 18—25 aprelya 2005 g.

5. Ob utverzhdenii Doktriny informacionnoj bezopasnosti Rossijskoj Federacii : Ukaz Prezidenta Rossijskoj Federacii ot 05.12.2016 № 646 [Ehlektronnyj resurs] // Informacionno-pravovoj portal GARANT.RU. — URL: http://www.garant.ru/products/ipo/prime/doc/71456224/ (data obrashcheniya: 16.06.2017).

6. Vekhov, V. B. Osobennosti rassledovaniya DDoS-atak, sovershennyh na web-servery organizacij / V. B. Vekhov // Problemy bor'by s prestupnost'yu: rossijskij i mezhdunarodnyj opyt : sb. nauch. tr. — Volgograd : VA MVD RF, 2009. — Vyp. 1. — S. 25—34.

7. Putin: FSB zafiksirovala za god 24 milliona atak hakerov na sajty gosorganov [Ehlektronnyj resurs] // TV-Centr. — URL: http://www.tvc.ru/news/show/id/87426 (data obrashcheniya: 16.06.2017).

8. FSB pomogla rossijskim bankam nejtralizovat' kiberataki v noyabre 2016 goda [Ehlektronnyj resurs] // INTERFAX.RU. — URL: http://www.interfax.ru/russia/547287 (data obrashcheniya: 16.06.2017).

9. Rossiya stala vtoroj posle SSHA po kolichestvu kiberatak [Ehlektronnyj resurs] // SorokaInfo.com. — URL: http://sorokainfo.com/news/rossija_stala_vtoroj_posle_ssha_po_kolichestvu_kiberatak/2017-06-13-3434 (data obrashcheniya: 16.06.2017).

10. Sberbank: poteri ot kiberugroz v mire k 2018 godu mogut vyrasti v chetyre raza [Ehlektronnyj resurs] // TASS. — URL: http://tass.ru/ekonomika/3355825 (data obrashcheniya: 16.06.2017).

11. Otchet Centra monitoringa i reagirovaniya na komp'yuternye ataki v kreditno-finansovoj sfere Glavnogo upravleniya bezopasnosti i zashchity informacii Banka Rossii za period s 01 iyunya 2015 goda po 31 maya 2016 goda [Ehlektronnyj resurs] // Central'nyj Bank Rossijskoj Federacii : oficial'nyj sajt. — URL: http://www.cbr.ru/credit/Gubzi_docs/fincert_survey.pdf (data obrashcheniya: 16.06.2017).

12. Kozlova, N. Obman valyut [Ehlektronnyj resurs] / N. Kozlova // Rossijskaya gazeta. — Federal'nyj vypusk № 6874 (6). — URL: http://rg.ru/2016/01/15/bastrykin.html (data obrashcheniya 16.06.2017).

13. O sozdanii gosudarstvennoj sistemy obnaruzheniya, preduprezhdeniya i likvidacii posledstvij komp'yuternyh atak na informacionnye resursy Rossijskoj Federacii : Ukaz Prezidenta Rossijskoj Federacii ot 15.01.2013 № 31s [Ehlektronnyj resurs] // Prezident Rossii : oficial'nyj sajt. — URL: http://www.kremlin.ru/acts/bank/36691 (data obrashcheniya 16.06.2017).

14. Vypiska iz Koncepcii gosudarstvennoj sistemy obnaruzheniya, preduprezhdeniya i likvidacii posledstvij komp'yuternyh atak na informacionnye resursy Rossijskoj Federacii (utv. Prezidentom Rossijskoj Federacii 12.12.2014 № K 1274) [Ehlektronnyj resurs] // Federal'naya sluzhba bezopasnosti Rossijskoj Federacii : oficial'nyj sajt. — URL: http://www.fsb.ru/files/PDF/Vipiska_iz_koncepcii.pdf (data obrashcheniya 16.06.2017).

15. Vekhov, V. B. Ponyatie, vidy i osobennosti fiksacii ehlektronnyh dokazatel'stv / V. B. Vekhov // Rassledovanie prestuplenij: problemy i puti ih resheniya. — 2016. — № 1. — S. 155—158.