DOI: 10.17117/na.2015.09.1218

Поступила (Received): 26.09.2015

<http://ucom.ru/doc/na.2015.09.1218.pdf>

Саганов П.Н.

Актуальные вопросы обеспечения национальной безопасности России от современных киберугроз

Saganov P.N.

Topical issues of ensuring national security of Russia from contemporary cyber threats

Научная статья посвящена проблеме обеспечения национальной безопасности Российской Федерации от реальных и потенциальных киберугроз, возникающих в современном мире. Автором предлагается комплекс мер правового, кадрового и организационно-технического характера по противодействию компьютерной преступности и совершенствованию информационной безопасности как важной составляющей национальной безопасности России

Ключевые слова: национальная безопасность, информационная безопасность, киберугрозы, компьютерная преступность, киберпреступность

The scientific article is devoted to the problem of ensuring the national security of the Russian Federation real and potential cyber-threats arising in the modern world. The author offers the complex of measures of legal, human, organizational and technical nature of anti-computer crime and improvement of information security as an important component of national security of Russia

Key words: national security, information security, cyber threats, computer crime, cyber crime

Саганов Петр Николаевич

Студент

Иркутский юридический институт (филиал)

г. Иркутск, ул. Шевцова, 1

Saganov Peter Nikolaevich

Student

Irkutsk law institute (branch)

Irkutsk, Shevtsova st., 1

С возникновением и стремительным развитием телекоммуникационных технологий пришла эра новой войны, действия, на фронтах которой продолжаются и в мирное время. С ростом популярности Интернета, использование такой сети как информационного оружия стало набирать обороты. Благодаря многомиллионной аудитории, доступности и простоте функционирования сети, Интернет превратился в поле брани, на котором в основном страдают рядовые пользователи, но зачастую представляет угрозу для целых государств.

Еще в 2009 году заместитель начальника Генерального штаба Вооруженных Сил Российской Федерации генерал-полковник Анатолий Ноговицын заявил, что наиболее развитые страны мира в ближайшие два-три года получат возможность вести полномасштабные войны в информационной сфере, он указал, что основными задачами в информационных войнах будут дезорганизация функционирования ключевых военных, промышленных, административных объектов и систем противника, а также информационно-

психологическое воздействие на его военно-политическое руководство, войска и население, прежде всего с использованием современных информационных технологий и средств. Так, по его словам, можно выделить ряд характерных черт информационной войны, которые отличают ее от других форм ведения военных действий, ставят новые проблемы перед ее участниками и заслуживают особого внимания. Основной из них являются незначительные затраты на разработку и применение информационного оружия, так как стоимость разработки высококачественных средств ведения информационной войны относительно невелика и доступна широкому кругу ее участников, повышение роли управления восприятием. Разрабатываемые средства «информационной войны» могут стать совершенно новым мощным инструментом манипуляции восприятием [1, с.23-25].

Примерами применения «кибероружия» могут служить обнаруженный в 2010 г., в локальной сети Бушерской АЭС в Иране, компьютерный червь «Stuxnet», который вывел из строя центрифуги электростанции; вирус-троян «Wiper» который в апреле 2012 г. уничтожил базы данных в десятках организаций Ирана, в т.ч. крупнейшего в Иране нефтяного терминала, работа которого была остановлена на несколько дней [с. 37].

Исходя из вышеизложенного, мы можем смело судить о том, что одной из причин ведения информационной войны (кибервойны) является достижение государством политических целей для оказания информационного давления или пропаганды, путем получения контроля над электронными и цифровыми средствами массовой информации, компьютерного шпионажа, вывода строя средств связи и массовых коммуникаций потенциального противника и иного причинения вреда противоборствующей стороне.

Таким образом, на современном этапе развития российского общества важное значение приобретают проблемы обеспечения его безопасности в целом и информационной безопасности в частности.

В связи с вышесказанным, следует отметить, что Российская Федерация не может игнорировать существующие угрозы использования кибероружия в целях обеспечения своей национальной безопасности.

Несмотря на уже принятые меры информационной безопасности, авторы полагают, что для охраны прав и законных интересов обладателей компьютерной информации и операторов информационных систем, необходимо усовершенствовать уголовное законодательство РФ, а именно в диспозицию ст. 273 УК РФ включить такое деяние как приобретение компьютерных программ либо компьютерной информации заведомо предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации, поскольку большинство преступников использующих вредоносные компьютерные программы не являются их создателями, а приобретают у представителей хакерского сообщества. Данная точка зрения высказывалась рядом авторов [2, с. 26; 5, с. 98], но законодательного закрепления до сих пор не нашла.

Целесообразно также учесть политические мотивы компьютерной преступности и дополнить диспозиции ч.3 ст.272, ч.2 ст.273, ч.1 ст.274 УК РФ но-

вым 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», справедливо, учитывая повышенную общественную опасность указанных преступных деяний, которые представляют собой ни что иное как «кибертерроризм» и должны наказываться более сурово, увеличить уголовную ответственность за такие преступные деяния [4, с. 108].

Следует отметить, что в юридической науке высказывалась точка зрения о возможности создания единого федерального органа исполнительной власти, занимающегося вопросами борьбы с преступлениями в информационной сфере, включая обеспечение безопасности информационной инфраструктуры критически важных и особо опасных объектов, а также воздействие на информационные инфраструктуры противника [1, с. 23-25].

Представляется, что создание самостоятельного государственного органа является излишним, но следует сформировать соответствующие подразделения в составе Федеральной службы безопасности РФ, Следственном комитете РФ, Министерстве обороны РФ (в МВД РФ данным подразделением является Управление «К»). При этом, требуется внести изменения в ст. 151 УПК РФ и отнести преступления, предусмотренные ч. ч. 2, 3, 4 ст. 272, ч. ч. 2, 3 ст. 273, ч. ч. 1, 2 ст. 274 УК РФ к подследственности органов Федеральной службы безопасности РФ.

Кроме того, авторы полагают, что на федеральном, региональном и муниципальном уровне, необходимо создание молодежных общественных движений из числа школьников, учащихся, студентов, целью которых являлся бы мониторинг российского сегмента информационной сети «Интернет» и выявление веб-сайтов, страниц, форумов экстремистской, террористической и иной криминальной направленности (детская порнография, продажа наркотических средств и психотропных веществ, организация и проведение азартных игр, суицид и пр.). Молодежь в данное время является самой большой интернет-аудиторией, поэтому ее взаимодействие с правоохранительными органами, органами государственной власти (Министерство связи и массовых коммуникаций Российской Федерации, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций и др.), органами местного самоуправления могло бы внести неоценимый вклад в противодействие компьютерной преступности и обеспечение национальной безопасности России от существующих киберугроз, в условиях информационных войн и конфликтов в киберпространстве.

Список используемых источников:

1. Бегишев И.Р. Информационное оружие как средство совершения преступлений // Информационное право. 2010. № 4. С. 23-25.
2. Евдокимов К.Н. Актуальные вопросы уголовно-правовой квалификации преступлений в сфере компьютерной информации // Российский следователь. 2015. № 10. С. 24-29.

3. Евдокимов К.Н. Причины компьютерной преступности в современной России // Российский следователь. 2015. № 10. С. 33-37.
4. Липинский Д.А., Евдокимов К.Н. Политические причины как современные факторы эволюции компьютерной преступности в Российской Федерации // Криминологический журнал Байкальского государственного университета экономики и права. 2015. Т. 9. № 1. С. 101-110.
5. Максимов В.Ю. Незаконные обращение с вредоносными программами для ЭВМ: проблемы криминализации, дифференциации ответственности и индивидуализации наказания :дисс. ... канд. юрид. Наук: 12.00.08. Краснодар: РГБ, 1998. 169 с.

© 2015, Саганов П.Н.

Актуальные вопросы обеспечения национальной безопасности России от современных киберугроз

© 2015, Saganov P.N.

Topical issues of ensuring national security of Russia from contemporary cyber threats