УДК 343.34:004.77

Бураева Людмила Александровна

**кандидат физико-математических наук,
доцент кафедры действия ОВД в особых условиях
Северо-Кавказского института повышения
квалификации (филиала)
Краснодарского университета МВД России**

О НЕКОТОРЫХ ВОПРОСАХ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ

Аннотация:
В статье рассмотрены актуальные вопросы обеспечения кибербезопасности в современных условиях, которые затрагивают широкий круг не только частных и корпоративных, но и государственных интересов, имеют широкое распространение и приобретают угрожающий характер. Приведен правовой аспект вопросов обеспечения кибербезопасности в Российской Федерации, обозначены главные тенденции развития киберугроз в современном глобальном информационном пространстве и меры, необходимые для их нейтрализации.

Ключевые слова:
кибербезопасность, киберугроза, глобальное информационное пространство, информационная безопасность, кибератака, кибертерроризм, киберпреступления, киберпреступники, вредоносное программное обеспечение.

Burayeva Lyudmila Aleksandrovna

**Assistant Professor, Department for Police Special Environment Operations,
North Caucasus Institute for Advanced Training,
branch of Krasnodar University of
the Ministry of Internal Affairs of Russia**

CONCERNING SOME ISSUES OF CYBER SECURITY IN MODERN CONDITIONS

Summary:
The article deals with the urgent issues of cyber security in modern conditions, which affect not only a wide range of private and corporate interests, but also public ones, and have become widespread and rampant. The author considers the legal aspect of the cyber security issues in the Russian Federation, discusses the main trends of the cyber threats evolution in the contemporary global information space and the measures necessary for their neutralization.

Keywords:
cyber security, cyber threat, global information space, information security, cyber attacks, cyber-terrorism, cyber-crimes, cyber criminals, malicious software.

Сегодня вопросы обеспечения кибербезопасности затрагивают все мировое сообщество. Глобальное информационное пространство, являясь совокупностью информационных ресурсов и инфраструктур, составляющих как государственные и межгосударственные компьютерные сети, телекоммуникационные системы и сети общего пользования, так и иные трансграничные каналы передачи информации, на данный момент насчитывает около 3,2 млрд пользователей [1]. Уже в 2016 г. число использующих глобальную сеть, по прогнозам аналитиков, увеличится примерно до 3,4 млрд, что будет составлять около 45 % населения нашей планеты. Причем Россия на сегодня по количеству интернет-пользователей занимает шестое место в мире и первое место в Европе, опередив Германию. По итогам 2014 г. рост по данному показателю в РФ составил 4 млн пользователей. Но, являясь, с одной стороны, несомненным достижением современности, глобальная сеть, с другой стороны, стала благодатной почвой для совершения так называемых компьютерных или киберпреступлений. Сегодня достаточно непросто обобщить существующие компьютерные преступления в силу их чрезвычайной многогранности и сложности. Преступления, совершаемые в глобальном информационном пространстве, затрагивают широкий круг не только частных и корпоративных, но и государственных интересов, имеют широкое распространение и приобретают угрожающий характер.

Само понятие «кибербезопасность» интегрирует в себе множество проблем различного типа, среди которых защита: данных и компьютерных систем, канала передачи данных, глобальной сети Интернет, телекоммуникационной инфраструктуры, основных услуг, приложений и другие. Однако следует заметить, что в российских нормативно-правовых документах и научной литературе чаще используется близкое по смыслу понятие «информационная безопасность», которое характеризует все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки. Следует отметить, что, по мнению аналитиков, основной целью атак являются не только информационные данные, но и технические и программные средства, формирующие информационно-телекоммуникационную инфраструктуру и цифровые системы управления, вследствие чего термин «кибербезопасность» и сопряженные с ним понятия, такие как «киберугроза», «киберпространство», «кибероружие», «кибератаки»,

«кибертерроризм» и т. п., требуют осмысления и формализации в виде понятийного аппарата. В настоящее время данные вопросы являются областью активных исследований и разработок, причем многие из них требуют комплексного подхода [2].

В начале 2014 г. Советом Федерации для всеобщего обсуждения был предложен проект Концепции стратегии кибербезопасности Российской Федерации, в котором определены направления усилий государства в отношении новых угроз, возникающих в современном информационном мире [3]. В проекте Концепции отмечено, что в настоящее время в Российской Федерации принят ряд документов, направленных на обеспечение различных аспектов национальной информационной безопасности [4; 5], однако они не охватывают в необходимой мере систему отношений, возникающих в рамках киберпространства как элемента информационного пространства. В проекте Концепции [6] даны определения таких понятий, как «информационное пространство», «информационная безопасность», «киберпространство» и «кибербезопасность», которая определена как совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями. В настоящее время продолжается активное обсуждение проекта, причем многие эксперты настаивают на необходимости доработки данного документа, имеющего столь важное значение для национальной безопасности страны, и указывают на необходимость дальнейшей методологической работы по определению основных понятий.

На данный момент среди главных тенденций развития киберугроз можно назвать следующие: стремительное увеличение числа кибератак, многие из которых ведут к большим потерям; повышение сложности атак, которые могут не только включать несколько этапов, но и использовать специальные методы защиты от их нейтрализации; воздействие почти на все электронные (цифровые) устройства, в частности на мобильные устройства, которые в наибольшей степени подвержены несанкционированному доступу; стремительный рост числа атак на информационную инфраструктуру крупных корпораций, значимых промышленных объектов, государственных структур; использование странами, развитыми в области компьютерных технологий, средств и методов кибернападения на другие государства. Перечисленные угрозы, подстерегающие нас в глобальном информационном пространстве, подтверждаются многочисленными сводками новостей, в которых сообщается о все новых фактах совершения киберпреступлений.

Ежегодно в глобальной сети обнаруживаются миллиарды вредоносных объектов, причем с каждым годом их число увеличивается примерно на 40 %. Ущерб от вредоносных атак в информационном пространстве оценивается в 100 млрд долл. США. По данным аналитиков каждую секунду жертвами киберпреступников становятся примерно 12 человек на Земле. Как правило, наиболее успешные атаки хакеров направляются на серверы и компьютеры конечных пользователей, подключенные к глобальной сети. Обычно для кибератак используются следующие инструменты: вредоносное программное обеспечение, троянские кони, бот-сети, фишинг, распределенные атаки типа «отказ в обслуживании», «человек посередине».

В настоящее время к устройствам наиболее высокой степени уязвимости в плане информационной безопасности относятся мобильные устройства. Повсеместно используемая программная платформа для мобильных устройств Android, доля которой на рынке составляет около 80 %, основана на «открытом» коде, подконтрольном специальным службам США. Данное явление создает реальную угрозу для национальной безопасности страны, переводя ее под контроль иностранных спецслужб. При этом доля разрабатываемых вредоносных программ для операционной системы Android, нацеленных на Android-устройства, стремительно растет. К концу 2012 г. доля вирусов для цифровых устройств на базе ОС Android составила почти 94 % среди общего количества вирусов для остальных мобильных ОС. Затем вредоносное программное обеспечение используется для скрытой установки на мобильные устройства с целью слежки за людьми, пользующимися современными средствами связи. При этом, по данным издания Wall Street Journal, ФБР располагает технологиями, которые позволяют удаленно включать микрофон на смартфонах и планшетах под управлением операционной системы Android и вести запись. То есть фактически мобильный телефон превращается в жучок, который пользователи носят при себе повседневно. Тревогу по данному вопросу уже забили власти КНР, которые усмотрели национальную угрозу в платформе Android.

Обеспечение кибербезопасности в данном направлении состоит в развитии производства электронных изделий и каналов сбыта инфокоммуникационных решений внутри страны. В целях комплексного решения проблемы необходимо организовать ряд системных НИОКР среди компетентных предприятий для обеспечения вывода на рынок востребованных продуктов мирового уровня. Это позволит государству на федеральном уровне сформировать защищенную инфраструктуру кибербезопасности и обеспечить развитие экономики на основе производства отечественных инфокоммуникационных решений.

Важной составляющей в вопросах обеспечения кибербезопасности является защита значимых государственных и промышленных объектов, нападения на которые участились в последнее время. Много шума наделали черви Stuxnet, Duqu и Flame, которые способны проникать в промышленные системы управления и изменять их код таким образом, чтобы атакующий мог перехватить управление ими без ведома операторов. Таким образом, можно привести в негодность заводы и даже атомные электростанции. К примеру, программа Stuxnet успешно вывела из строя 80 % иранских центрифуг по обогащению урана. Причем стало известно о причастности специалистов американских спецслужб к созданию указанных комплексных вредоносных программ, при этом финансирование нападений в области киберпространства ведется государственными структурами США.

Ежегодно фиксируются многочисленные атаки на крупнейшие банки мира. В октябре 2014 г. была выявлена вредоносная сеть из более чем 500 000 компьютеров, которая использовала контрольную панель на удаленном сервере для сбора воруемых данных. Таким образом было похищено почти 800 000 собранных пар логин-пароль, многие из которых были действующими и привязаны к системам онлайн-банкинга европейских и американских банков [7]. В феврале 2015 г. стало известно о хакерской операции Carbanak, в ходе которой киберпреступники украли около миллиарда долларов из 100 финансовых организаций, принадлежавших почти 30 странам мира. Каждая кибератака приносила киберпреступникам до 10 млн долл., причем от первого проникновения до вывода денег из системы у компьютерных мошенников уходило от двух до четырех месяцев. Вывод денег осуществлялся через онлайновые платежные системы [8]. Специалисты полагают, что за операцией стоит международная группировка, включающая киберпреступников из России, Украины, ряда европейских стран, а также Китая.

Все большие обороты набирают преступления террористической и экстремистской направленности [9; 10; 11] в сети Интернет. Уже к 1998 г. примерно 30 террористических организаций имели свои интернет-сайты, в настоящее время в мировой сети представлены все активно действующие террористические и экстремистские организации [12], при этом многие из них имеют более одного сайта на нескольких языках.

Все чаще глобальное информационное пространство используется для хищения государственных секретов. Так, в 2013 г. «Лабораторией Касперского» была раскрыта шпионская сеть под названием «Красный Октябрь» («Red October»), которая на протяжении пяти лет занималась хищением государственных секретов. Данная сеть представляла собой сложнейший комплекс вредоносных программ, которыми были заражены компьютеры различных государственных структур, посольств, секретных научных институтов и прочих организаций. Шпионской сетью были охвачены бывшие республики СССР, почти вся Западная Европа, Австралия и США. Комплексное шифрование с использованием алгоритмов SSL / TLS является широко известной технологией, с помощью которой можно решить обозначенную проблему. Однако криптографическая защита информации не применяется повсеместно по различным причинам, среди которых: организационная инертность, неграмотность, плохая информированность.

В конце 2012 г. свои подозрения публично высказали американские и китайские государственные структуры, выдвинув обвинения в создании оборудования с недокументированными возможностями, с помощью которого в будущем будет осуществляться кибератака другой страны. Предположительно нападения чаще всего организуются из Китая [13]. Активное участие государственных структур развитых стран в сборе информации о гражданах, чиновниках, корпорациях и других важных сведений, которые в будущем можно использовать для достижения кумулятивного эффекта и получения закрытой информации, подтверждаются неоднократными заявлениями Эдварда Сноудена.

Правовая база противодействия киберугрозам в России последовательно развивается с 2000 г., когда была принята Доктрина информационной безопасности Российской Федерации. С 2008 г. действует Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена». В 2013 г. утверждены «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г.». В ноябре 2013 г. Совет Федерации проводил слушания, на которых обсуждался проект Концепции стратегии кибербезопасности Российской Федерации, который был выставлен для общественного обсуждения на сайте Совета Федерации.

Однако проблемы, имеющиеся в сфере обеспечения кибербезопасности на современном этапе, не могут быть полноценно решены традиционными средствами и требуют системного подхода при создании комплексной системы безопасности, способной противостоять многочисленным киберугрозам. Речь идет о координации усилий в данном направлении государственных органов,

бизнеса и общества в целом. При этом полноценно и гарантированно решать вопросы кибербезопасности можно только тогда, когда в нашей стране будет использоваться российское телекоммуникационное оборудование, программное обеспечение, средства защиты информации.

Ссылки:

1. Бураева Л.А. Террористические объединения в глобальном информационном пространстве // Пробелы в российском законодательстве. 2014. № 3. С. 274–276.
2. Безкоровайный М.М. Кибербезопасность подходы к определению понятия // Вопросы кибербезопасности. 2014. № 1 (2). С. 22–27.
3. Концепция стратегии кибербезопасности Российской Федерации [Электронный ресурс] : проект. URL: http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 17.06.2015).
4. Стратегия развития информационного общества в Российской Федерации : утв. Президентом РФ В.В. Путиным от 7 февраля 2008 г. № Пр-212 // Российская газета. 2008. 16 февр.
5. Доктрина информационной безопасности Российской Федерации : утв. Президентом РФ В.В. Путиным 9 сентября 2000 г. № Пр-1895 // Российская газета. 2000. 28 сент.
6. Концепция стратегии кибербезопасности …
7. Выявлена вредоносная сеть из более чем 500 000 компьютеров [Электронный ресурс]. URL: http://www.cybersecurity.ru/crypto/197482.html (дата обращения: 17.06.2015).
8. Хакеры украли миллиард долларов в ходе крупнейшей атаки на банки [Электронный ресурс]. 2015. 16 февр. URL: http://lenta.ru/news/2015/02/16/yardhack/ (дата обращения: 04.07.2015).
9. Шхагапсоев З.Л., Тарчоков Б.А. Современные контуры системы противодействия различным проявлениям терроризма : учеб. пособие. Нальчик, 2012. 136 с.
10. Гаужаева В.А. Признаки терроризма, формирующие его понятие в нормативных и научных источниках // Актуальные вопросы юридических наук в современных условиях : сб. науч. тр. по итогам междунар. науч.-практ. конф. СПб., 2015. С. 69–72.
11. Карданов Р.Р. Роль судебно-криминалистических экспертиз в антитеррористической деятельности // Доклады Адыгской (Черкесской) Международной академии наук. 2014. Т. 16, № 1. С. 92–96.
12. Бураева Л.А. Информационные войны и информационный терроризм в современном мире: методы и поле действия // Известия Кабардино-Балкарского научного центра РАН. 2014. № 1. С. 7–11.
13. «Лаборатория Касперского» раскрыла шпионскую сеть «Red October» [Электронный ресурс]. URL: http://24gadget.ru/1161053174-laboratoriya-kasperskogo-raskryla-shpionskuyu-set-red-october.html (дата обращения: 17.06.2015).

References:

1. Buraeva, LA 2014, ‘The terrorist association in the global information space’, *Gaps in Russian legislation,* no. 3, p. 274-276.
2. Bezkorovainy, MM 2014, ‘Cybersecurity approaches to the definition’, *Cybersecurity,* no. 1 (2), p. 22-27.
3. *The concept of cyber-security strategy of the Russian Federation: the project* 2015, retrieved 17 June 2015, <http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf>.
4. ‘Strategy for Information Society Development in the Russian Federation approved by Russian President VV Putin, on February 7, 2008 № Pr-212’ 2008, *Russian newspaper,* Feb. 16.
5. ‘Information Security Doctrine of the Russian Federation approved by Russian President VV Putin, September 9, 2000 № Pr-1895’ 2000, *Russian newspaper,* Sep. 28.
6. *The concept of cyber-security strategy of the Russian Federation: the project* 2015, retrieved 17 June 2015, <http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf>.
7. *Revealed malicious network of more than 500,000 computers* 2015, retrieved 17 June 2015, <http://www.cybersecurity.ru/crypto/197482.html>.
8. *Hackers stole a billion dollars in the largest attack on the banks* 2015, Feb. 16, retrieved 04 July 2015, <http://lenta.ru/news/2015/02/16/yardhack/>.
9. Shhagapsoev, ZL & Tarchokov, BA 2012, *The modern contours of countering the various manifestations of terrorism,* Nalchik, 136 p.
10. Gauzhaeva, VA 2015, ‘Signs of Terrorism, forming the concept in its regulatory and scientific sources’, *Actual questions of legal science in modern conditions: scientific works on the results of Intern. scientific and practical Conf.,* St. Petersburg, p. 69-72.
11. Kardanov, RR 2014, ‘Role of Forensic Expertise in anti-terrorist activities’, *Reports of the Adyghe (Circassian) International Academy of Sciences,* vol. 16, no. 1, p. 92-96.
12. Buraeva, LA 2014, ‘Information war and information terrorism in the world today: methods and field of action’, *Proceedings of the Kabardino-Balkar Scientific Centre of Russian Academy of Sciences,* no. 1, p. 7-11.
13. *"Kaspersky Lab" uncovered a spy network «Red October»* 2015, retrieved 17 June 2015, <http://24gadget.ru/1161053174-laboratoriya-kasperskogo-raskryla-shpionskuyu-set-red-october.html>.