3. Научно-практический комментарий к Уголовному кодексу Республики Беларусь : [с учетом изменений и дополнений по состоянию на 23 февраля 2010 г.] / Н.Ф. Ахраменка [и др.] ; под ред. А.В. Баркова, В.М. Хомича. – Минск : Гос ин-т управления и социальных технологий Белорусского государственного университета, 2010. – 1063 с.
4. Уголовное дело по факту оскорбления в сети интернет возбуждено в Витебской области [Электронный ресурс] / Новости Беларуси. – Режим доступа: http://www.belta.by/ru/all_news/incident?id=681796. – Дата доступа: 14.04.2015
5. Чередниченко, Е.Е. Клевета и оскорбление: уголовно-правовой анализ (проблемы теории и практики) : моногр. / Е.Е. Чередниченко. – М. : Издательство «Юрлитинформ», 2010. – 144 с.

УДК 343.3/.7

«КИБЕРВОЙНА» КАК НОВЫЙ ВИД ВЫСОКОТЕХНОЛОГИЧЕСКОЙ ВОЙНЫ

Д.С. МАЛИНИНА
(Представлено: Т.И. ПУГАЧЁВА)

Дается определения терминам «кибервойна», «киберугроза», «кибероружие». Кибернетика как основоположник «кибервойны». Киберугрозы создают хакеры, люди способные взламывать серверы и получать из них информацию незаконным путем. Кибероружия подводят общедоступные утилиты работы с сетевой инфраструктурой и нагрузочного тестирования сетей на основании того, что их используют хакеры.

В последнее время все чаще в средствах массовой информации (далее – СМИ) используются термины «кибероружие», «киберугроза», и «кибервойна». Это происходит в основном из-за того, что журналисты быстро подхватили не самый удачный термин, используя его в отрыве от контекста. В результате кибервойной с равной вероятностью могут называться пропагандистские операции в информационном пространстве Интернета, попытки взлома банковских систем, операции по выведению из строя критической информационной инфраструктуры, а также любые действия, которые прямо или косвенно связаны с Интернетом, компьютерами и т.п. Точно так же размыто и понятие «киберугроза»: под него зачастую бездумно подводятся опасности, такие, как распространение определенных видов информации в сети, вопросы обеспечения безопасности информационных систем, противостояния вредоносному программному обеспечению (далее по тексту – ПО) и многое другое [1 с. 72].

Настоящая научная статья ставит перед собой целью дать определение термину «кибервойна». Но для того, что бы дать определение всем этим термина, необходимо разобрать основоположника этих терминов «кибернетика».

Термин «кибернетика» появился еще в 1830 г. в философских трудах Андре-Мари Ампер [2], который более известен как один из пионеров электродинамики. Кибернетика определялась Ампером как наука о рациональном управлении государством. В 1948 г. понятие «кибернетика» было использовано Норбертом Винером как наименование науки о закономерностях процессов управления и передачи информации в машинах, живых организмах и в обществе [3] . Объектом исследования кибернетики являются все без исключения управляемые системы, которым присуща обратная связь. Иными словами, кибернетика вовсе не ограничена исследованиями современных информационных систем, алгоритмов и протоколов. Будучи междисциплинарной наукой, она охватывает системы электрических цепей, технологические процессы, логистику, эволюционную биологию, психологию личности, социологию, синергетику и т.п. Особо отметим то, что кибернетика, как наука об управлении, уделяет самое пристальное внимание методам управления государством и обществом. Именно эта область внимания кибернетики и стала причиной ее критики в СССР с последующим объявлением «реакционной лженаукой» в 1950-х гг. Кибернетика, как тогда казалось, претендовала на разработку научно обоснованного аппарата управления государством, стремилась «отбросить современную научную мысль, основанную на материалистической диалектике». Между тем наиболее интересные исследования кибернетиков относились именно к исследованиям государства в целом так и определенные аспекты (общества, политику и как способ административного управления). В области исследований информационных систем на смену «общей» кибернетике был создан специализированный высокоэффективный математический аппарат, опирающийся на хорошо разработанные теории систем, управления, автоматов, алгоритмов и т.п. В практическом решении прикладных задач, связанных с информационными технологиями, как правило, используется именно этот аппарат, а не «общая» кибернетика [1].

Под термином «кибероружие» в настоящее время понимаются самые разнообразные технические и программные средства, чаще всего направленные на эксплуатацию уязвимостей в системах передачи и

обработки информации или программотехнических системах. Так, под определения кибероружия подводят общедоступные утилиты работы с сетевой инфраструктурой и нагрузочного тестирования сетей на основании того, что их используют хакеры. Опираясь на масштабность воздействия, к кибероружию причисляют вирусы типа Flame [4] или зомби-сети, используемые для рассылки спама и организации распределенных атак, которые направлены на перегрузку информационных систем и следующий из нее отказ в обслуживании (DOS и dDOS-атаки) [5 с. 21] .

«Киберугроза» – это незаконное проникновение или угроза вредоносного проникновения в виртуальное пространство для достижения политических, социальных или иных, целей. Киберугроза может воздействовать на информационное пространство компьютера, в котором находятся сведения, хранятся материалы физического или виртуального устройства. Атака, обычно, поражает носитель данных, специально предназначенный для их хранения, обработки и передачи личной информации пользователя [6].

Киберугрозы создают хакеры, люди способные взламывать серверы и получать из них информацию незаконным путем. Хакер является высококвалифицированным специалистом в программировании. Так в настоящем времени их называют не иначе как «компьютерный злоумышленник».

Подводя итоги всему выше сказанному, нужно ответить на самый главный вопрос: «Так, что же такое «кибервойна»?

Кибервойна, Кибернетическая война (англ. Cyberwarfare) – информационное противостояние в киберпространстве, в том числе компьютерное противостояние в Интернете, одна из разновидностей информационной войны [10]. Она направлена прежде всего на дестабилизацию компьютерных систем и доступа к интернету государственных учреждений, финансовых и деловых центров и создание беспорядка и хаоса в жизни стран, которые полагаются на интернет в повседневной жизни. Межгосударственные отношения и политическое противостояние часто находит продолжение в интернете в виде кибервойны: вандализме, пропаганде, шпионаже и непосредственных атаках на компьютерные системы и сервера.

Одно из определений термина звучит так: «„кибервойна“ – использование Интернета и связанных с ним технологических и информационных средств одним государством с целью причинения вреда военной, технологической, экономической, политической, информационной безопасности и суверенитету другого государства» [11].

Как писал эксперт по безопасности правительства США Ричард Кларк в своей книге «Кибервойна» (англ. CyberWarfare) [12] (вышла в мае 2010 года) «кибервойна – действия одного национального государства с проникновением в компьютеры или сети другого национального государства для достижения целей нанесения ущерба или разрушения». Британский журнал The Economist описывает киберпространство как «пятую область войны, после земли, моря, воздуха и космоса» [13]. О важности готовности к ведению военных действий в киберпространстве свидетельствуют факты создания в 2005 году Агентства сетевой и информационной безопасности Евросоюза [14], а в 2010 году – специального формирования ВС США – киберкомандования США [15].

ЛИТЕРАТУРА

1. Каберник, В.В. Проблемы классификации кибероружия / В.В. Каберник // Вестн. МГИМО-Ун-та. – 2013. – № 2 (29) – С. 72–73.
2. Андре- Мари Ампер : биогр. [Электронный ресурс]. – Режим доступа: http:// www.people.su/5663. – Дата доступа: 26.09.2015.
3. Норберт Винер : биогр. [Электронный ресурс]. – Режим доступа: http://to-name.ru /biography/norbert-viner.htm. – Дата доступа: 26.09.2015.
4. Комплекс вредоносных программ, использовавшихся для осуществления шпионской деятельности на Ближнем Востоке [Электронный ресурс]. – Режим доступа: http://www.securelist. com/ru/blog/2077 64007/ The_Roof_Is_on_Fire_otklyuchenie_komandykh_serverov_Flame. – Дата доступа: 26.09.2015.
5. Анализ типовых нарушений безопасности в сетях. – СПб. : Вильямс, 2001. – 21 с.
6. Киберугроза [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru /news/ tags/%EA%E8%E1%E5%F0%F3%E3%F0% EE%E7% E0/. – Дата доступа: 26.09.2015.
7. Попов, И.М. Взгляд на действия в киберпространстве под военным углом зрения [Электронный ресурс]. – Режим доступа: http://www.milresource.ru/Cyber-Popov.html. – Дата доступа: 26.09.2015.
8. США разрабатывают наступательные кибероперации [Электронный ресурс]. – Режим доступа: http://www.belvpo.com/ru/18385.html. – Дата доступа: 26.09.2015.
9. Википедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/%D0% AD%D0%BA%D1%81%D0%BF%D0%BB%D0% E% D0% B9%D1%82. – Дата доступа: 26.09.2015.
10. Википедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/%D0 %9A%D0%B8% D0%B1%D0%B5%D1%80%D0%B2%D0%BE%D0%B9%D0%BD%D0%B0. – Дата доступа: 26.09.2015.
11. Конвенция о запрещении использования кибервойны [Электронный ресурс]. – Режим доступа: http://www.answerme.org/politik.org.ua. – Дата доступа: 26.09.2015.
12. Clarke, R.A. Cyber War [Электронный ресурс] / R.A. Clarke // Harper Collins. – Режим доступа: http://www.harpercollins.com/9780061962233/cyber-war. – Дата доступа: 26.09.2015.

13. Cyberwar: War in the Fifth Domain [Электронный ресурс] // Economist. – Режим доступа: http://www.economist.com/node/16478792. – Дата доступа: 26.09.2015.
14. European Union Agency for Network and Information Security [Электронный ресурс]. – Режим доступа: https://www.enisa.europa.eu/. – Дата доступа: 26.09.2015.
15. NSA chief may lose US Cyber Command role [Электронный ресурс]. – Режим доступа: http://www.cnet.com/news/nsa-chief-may-lose-us-cyber-command-role. – Дата доступа: 26.09.2015.

УДК 343.3/.7

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ – ЗАДАЧА МЕЖДУНАРОДНОГО УРОВНЯ

Д.С. МАЛИНИНА
(Представлено: Т.И. ПУГАЧЁВА)

Термин «кибероперация» в профессиональной военной среде. Ключевой категорией понятия «действия в киберпространстве в военных целях» является само киберпространство. Основные специалисты и средства, привлекаемые для проведения кибероперации. Мнению российских специалистов в области кибербезопасности.

Из-за участившихся в последние годы попыток несанкционированного вторжения в информационные и компьютерные сети и системы (в том числе оборонного значения) ряда стран Запада с целью их нарушения или блокирования предпринимаются определенные меры (наиболее энергичные в Соединенных штатах Америки (далее – США)) по нейтрализации этой очередной нетрадиционной угрозы национальной безопасности. К таким мерам относится, в частности, формирование в составе национальных ВС так называемых сил кибероперациий (СКбО), предназначенных для противоборства в информационном и киберпространствах [1].

Широко употребляемый термин «кибероперация» в профессиональной военной среде неизбежно вызывает ассоциации с понятием «военная операция», поэтому допустимость его употребления в военном лексиконе, очевидно, еще следует осмыслить.

В данном материале речь идет исключительно о военной сфере и вооруженных силах: хакерские атаки, подрывная и иная тайная деятельность спецслужб в киберпространстве, вирусы и DDOS-атаки нашего времени намеренно исключаются из сферы нашего внимания. Вооруженные силы будут вести реальные действия в киберпространстве в военных целях только с началом войны, а в мирное время они должны заниматься всесторонней подготовкой к их ведению, имея, кстати, в своем киберарсенале такие средства и способы действий, которые в мирное время могут даже квалифицироваться как негуманные, незаконные, катастрофические по последствиям.

Ключевой категорией понятия «действия в киберпространстве в военных целях» является само киберпространство. Однако у экспертов сегодня нет единого подхода к определению этого понятия. Авторская позиция заключается в том, что с военной точки зрения киберпространство представляет собой специфическую составную часть более широкого понятия – информационного или информационно-коммуникационного пространства, без которого сегодня уже немыслимы военные действия. В структурном отношении киберпространство включает в себя аппаратно-программные комплексы и объединяющие их компьютерные сети, в которых накапливается, хранится и циркулирует информация. Если прибегнуть к образному сравнению, то информационные потоки являют собой своеобразную «кровь» военного организма, а киберпространство в таком случае выступает в роли «кровеносной системы», которая наполнена той самой «кровью» – информацией [2].

Говорить о каком-либо самостоятельном значении киберпространства как обособленной сферы ведения войны или обособленного «театра военных действий» нельзя. Или по крайней мере еще преждевременно. В современной войне действия в киберпространстве будут иметь вспомогательный, подчиненный характер по отношению к военным (боевым) действиям.

В настоящее время одним из приоритетных направлений развития вооруженных сил США выделяется наращивание сил и средств для ведения информационной войны. Особую значимость здесь приобретает развитие киберподразделений, совершенствование методов и способов киберзащиты, а также проведение наступательных операций в киберпространстве.

Киберподразделение – это подразделение, которое нацелено на исследования и преследование по суду интернет-преступления, включая «киберосновaнный терроризм, шпионаж, компьютерные вторжения и главное кибер-мошенничество». В США возглавляет это подразделение Федерального бюро расследований (далее – ФБР). Так же в Республике Беларусь идет активная разработка и создание киберподразделения. В данный момент у нас уже существует (но, конечно же, не афишируется) киберподразделение при Министерстве обороны Беларуси.