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.

В данный момент американскими экспертами разработан наиболее вероятный сценарий проведения кибероперации, включающий три основных этапа.

На первом – скрытом этапе подготовки к проведению кибероперации – усилия специалистов направляются на выявление информационных объектов критически важной инфраструктуры атакуемого государства, внедрение оперативных сотрудников в учреждения с закрытыми системами управления (администрация президента или аппарат правительства, ключевые министерства, крупнейшие банки, нефтегазовые корпорации и т.п.), выявление уязвимостей в их системах безопасности и эксплуатируемом на объектах программном обеспечении, а также разработку вредоносного специального программного обеспечения (эксплойтов, уязвимостей «нулевого дня», программ удаленного управления и др.).

Активный этап подготовки к проведению кибероперации, как правило, включает создание ботнетов (заражение компьютеров), вторжение в закрытые информационные системы, а также актуализацию доступа к уже взломанным системам.

В ходе непосредственного проведения кибератаки осуществляется дезорганизация и вывод из строя систем государственного и военного управления, систем контроля движения транспорта, нарушение работы банков и бирж, отключение Интернета, сотовой связи и т.д. [4].

Так США идет работы над составлениями план по подготовки специалистов в области информационных технологий (таблица).

Таблица

Основные специалисты и средства, привлекаемые для проведения кибероперации
(по взглядам американских экспертов)

Специализация	Основные функции	Требования к уровню знаний специалиста в информационных технологиях	Примерное количество человек	Ориентированная заработная плата (долларов США в год)
1	2	3	4	5
Специалист по выявлению уязвимостей	Поиск известных дефектов безопасности и ранее неизвестных уязвимых мест в операционных системах, программах, браузерах, серверах, сетях, смартфонах	Мирового класса	10	250 000
		Студент факультета информатики	10	40 000
Разработчик эксплойто*	Создание вредоносных кодов, эксплуатирующих уязвимости компьютеров при их заражении	Морового класса	10	250 000
		С опытом использования спец. программ Студент факультета информатики	40 20	100 000 45 000
Коллектор ботов	Заражение чужого компьютера для превращения его в бот (компьютер-зомби)	Дипломированный специалист Студент факультета информатики	40 10	75 000 40 000
Специалист по поддержке ботнетов	Поддержка и управление сети ботов как внутри, так и вне атакуемой страны, мониторинг рынка антивирусов ПО	Дипломированный специалист	150	60 000
		Студент факультета информатики	20	45 000
Оперативные сотрудники	Поступление на работу в ключевые гражданские и военные учреждения и коммерческие организации, подготовка условий для атаки изнутри посредством получения доступа к закрытым системам и подключения их к Интернету с помощью беспроводного подключения	Опытные завербованные сотрудники	10	По договоренности
		Студенты факультета информатики	10	40 000
Операторы	Проникновение через установленное оперативными сотрудниками оборудование в закрытие системы, их изучение и взлом	Специалист по взлому систем Студенты факультета информатики	40 10	100 000 40 000

Окончание таблицы

1	2	3	4	5
Разработчики	Разработка средств дистанционного контроля зараженных компьютеров, подготовка DDoS атак	Опытный специалист	10	125 000
		Дипломированный специалист Студент факультета информатики	20 10	60 000 40 000
Тестеры	Проверка надежности и эффективности всех разработанных программ, ботнетов и средств дистанционного контроля	Дипломированный специалист	10	60 000
		Студент факультета информатики	5	40 000
Технический консультант	Эксперт по специализированному оборудованию и программному обеспечению		20	100 000
Системный администратор	Поддержка работоспособности систем, установка ПО		10	50 000
Старший менеджер	Управление персоналом		5	200 000
Менеджер	Управление «кибербойцами»		47	100 000

*Примечание : * компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему. Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение её функционирования (DoS-атака) [3].*

Что же по этому поводу горят российские специалисты? По мнению российских специалистов в области кибербезопасности, этот сценарий проведения кибероперации «является весьма реалистичным». В качестве основного аргумента приводится тот факт, что сегодня ключевые ведомства России (в частности министерства, курирующие вопросы экономики, промышленности, энергетики, силовые и другие структуры) используют технические средства и программное обеспечение зарубежного производства [4].

ЛИТЕРАТУРА

1. Каберник, В.В. Проблемы классификации кибероружия / В.В. Каберник. – Вестн. МГИМО-Ун-та. – 2013. – № 2 (29) – С. 72–73.
2. 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.
3. 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.
4. США разрабатывают наступательные кибероперации [Электронный ресурс]. – Режим доступа: http://www.belvpo.com/ru/18385.html. – Дата доступа: 26.09.2015.