ЛЕТОПИСИ КИБЕРВОЙН И ВЕЛИЧАЙШЕГО В ИСТОРИИ ПЕРЕРАСПРЕДЕЛЕНИЯ БОГАТСТВА

Рецензия на книгу Харриса Ш. «Кибер войн@. Пятый театр военных действий»

Марков А.С.

Введение

Несколько лет назад вице-премьер Д.О. Рогозин и министр обороны С.К. Шойгу объявили о создании в нашей стране киберкомандования. На усиление глобального информационного противоборства и противоправной деятельности в кибернетической области и в сфере высоких технологий указано и в новой Стратегии национальной безопасности РФ, утвержденной Президентом в предновогодний день.

Поэтому появление на российском рынке книги американского публициста Шейн Харрис про кибервойны весьма кстати. Книга включает 14 глав, которые насыщены пересказами нескольких сотен удивительных историй и индивидуальными интервью.

Однако детальное ознакомление с книгой показало, что она отличается высоколитературным слогом, зачастую отвлекающим от заявленной направленности издания. В этом плане книга, на наш взгляд, чуть проигрывает известным российскому читателю монографиям, подготовленным под руководством Р.А. Кларка [2] и С.А. Паршина [3], которые хорошо структурированы и подтверждены официальными источниками.

Целью данной рецензии стал анализ некоторых тенденций и ключевых факторов кибервойн на основе новых актуальных данных, представленных в указанной книге.

Ключевые моменты книги

В книге можно вычленить ряд ключевых информационных утверждений, к принятию которых Шейн Харрис последовательно склоняет читателей, а именно:

1) возрастающая роль кибероперaций в современной войне;

2) высокая степень уязвимости национальных информационных инфраструктур, в первую очередь критических;

3) неожиданная эффективность кибершпионажа в глобальном экономическом и политическом противостоянии;

4) рост технологической и киберэкспансии со стороны Китая;

5) последовательная и принципиальная позиция спецслужб США в отстаивании интересов ее национальной безопасности.

С самого начала книги очевидна озабоченность США относительно нарастающей активности Китая в киберпространстве, поэтому рассмотрим этот вопрос в первую очередь.

Китайская кибервойна как достижение политических целей

Достаточно просто пролистать книгу по диагонали, чтобы определить, кто «Мистер Зло» в киберпространстве с точки зрения США (рис.1 и 2).

Заметим, такая статистика разнится с имеющейся ранее [3, с.50].

Описывая акции китайских хакеров, автор подчеркивает, что их действия отличаются от кибератаки других государств и сообществ, а именно:

1) действия в киберпространстве носят амбициозный прагматический характер (достижения глобального экономического превосходства в течение одного поколения страны);

2) компьютерные атаки преимущественно характеризуются высоким уровнем технологичности и результативности в плане проникновения с целью сбора информации (т.е. мало касаются технологий прошлого века, как-то: DDOS-атаки или подмена контента).

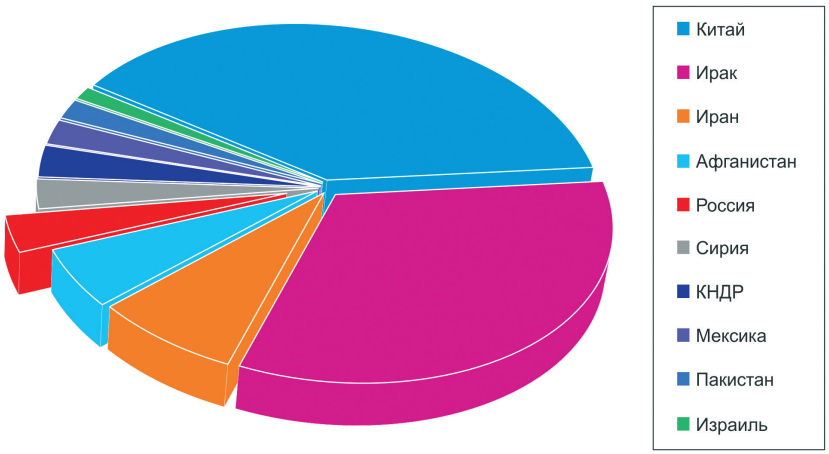


***Рис. 1**. Упоминаемые в киберакциях страны.*

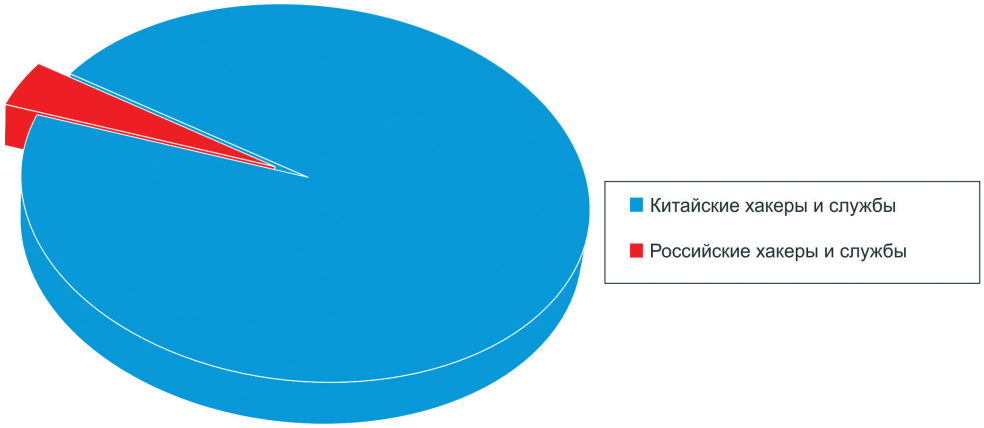


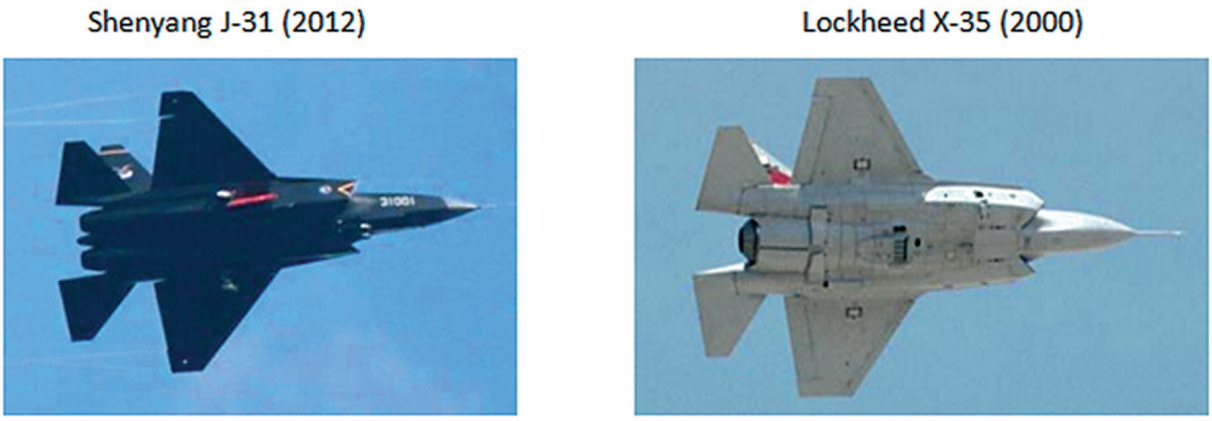
***Рис. 2.** Соотношение упоминаний китайских и российских участников киберакций.*

В качества впечатляющей победы КНР на полях киберпространства автор отмечает несанкционированное копирование конструкторской документации по единому ударному истребителю-бомбардировщику 5-го поколения Joint Strike Fighter F-35 (рис. 3). Писатель оценивает стоимость проекта в 337 млдр.$[1], при этом в результате китайских кибератак стоимость проекта была увеличена на 50%, а сроки проекта были существенно сдвинуты [1, с.18]. Автор констатирует, что вторжения касались не столько датацентров Пентагона, сколько информационной инфраструктуры исполнителей гособоронзаказа США, в том числе соисполнителей нижнего звена и всевозможных партнеров.

К блестящим достижениям китайской военной киберразведки автор (кроме компрометации JSF F-35), относит кражу документации по вертолету Black Hawk, стратегическому разведывательному БПЛА Global Hawk, ракетным системам Patriot, реактивным двигателям General Electric, системе ПРО Aegis, технологиям разведки мин, боевым кораблям прибрежной зоны (класса LCS), боевой машины морской пехоты, стратегическому военно-транспортному самолёту Boeing C-17 Globemaster (GAFMS), а также компрометацию схемотехнических решений для легких торпед (класса LHT), планов экипировки солдат системами наблюдения и разведки, технического проекта перспективного сверхбольшого грузового самолета, системного проекта самолета-разведчика RC-135 [1, с.219]. В интернет-сети можно также найти подобные ссылки про палубный истребитель F-18, противоракетный комплекс THAAD, конвертопланы V-22 Osprey и другие кибертрофеи.

Успехи промышленного кибершпионажа просто зашкаливают. Казалось бы, достаточно было бы упомянуть копирование исходных кодов сетеобразующих устройств компании Cisco (основ-

1 Для сравнения, что примерно соответствует ВВП 14-ти прибалтийских республик (2015 г.) или стоимости 3-х тринадцатилетних лунных программ «Аполлон» (в эквиваленте 2015 г.).



Источник: www.aihami.com

***Рис. 3**. Морфологическое сходство истребителей 5-го поколения США и КНР.*

ного поставщика минобороны США, DoD) и подозрения относительно процветания Huawei или же удивительную удачу китайской промышленности в выпуске солнечных батарей после взлома американской компании SolarWorld.

Однако автор методично перечисляет весьма большое количество фактов кражи интеллектуальной собственности США, касающихся, например:

- отчета Mandiant о компрометации 141 организаций китайскими хакерами в течение 2006-2013 гг. (рис.4.) [4];

- сообщения Google об операции Aurora в 2009 г.

- APT-атак на три сотни компаний США, включая Juniper Networks, Northrop Grumman, Yahoo, Symantec и Adobe Systems (последняя, кстати, заявила о хищении исходных кодов ее программных продуктов и данных 38 млн. ее клиентов).

Шейн Харрис предполагает, что компрометации подверглись тысячи корпоративных систем США.

Нельзя не процитировать слова директора Агентства национальной безопасности США (NSA, подразделение DoD) Александера К.Б., который охарактеризовал «необузданный промышленный шпионаж, проводимый Китаем, **величайшим в истории перераспределением богатства**» [1, с.100].

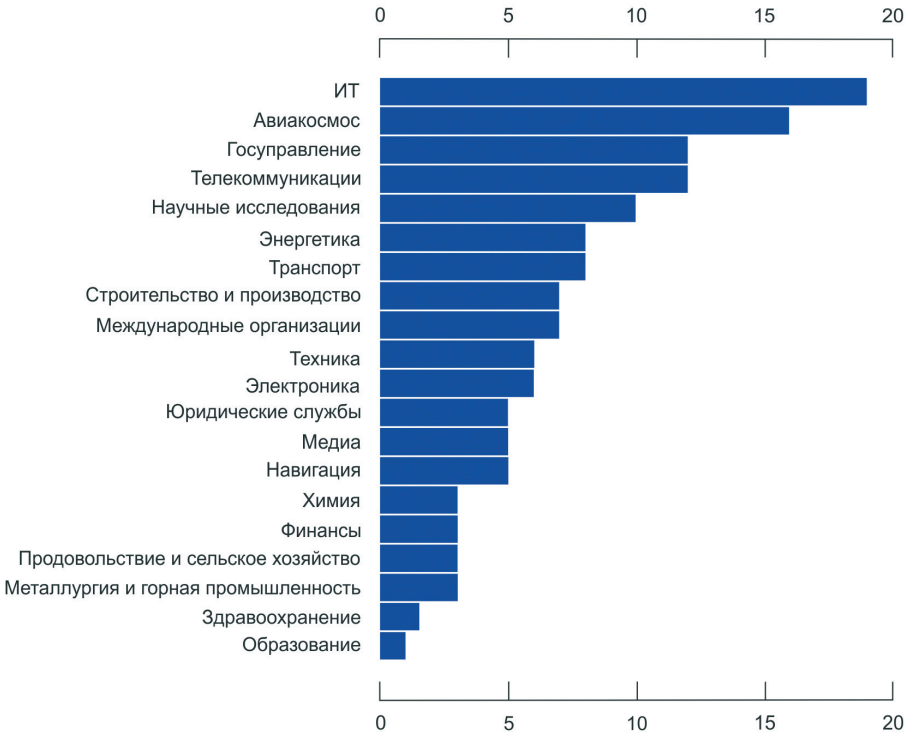


***Рис. 4**. Статистика по компрометации организаций [4].*

Рис.5. *Модель жизненного цикла APT-атаки [4].*

Так как книга вышла в США в 2014 г., автор не успел добавить американо-китайские скандалы 2015 года, как-то: взлом 700 порталов НИИ и предприятий промышленности США, компрометацию медицинских данных 80 млн. граждан США, компрометацию около 40 млн. персональных данных госслужащих США (атака на Office of Personnel Management), имеющих доступ к гостайне, и членов их семей, включая личные дела сотрудников спецслужб, в том числе 5,6 млн. их электронных отпечатков данных и др.[2] Особенно нелицеприятным видится сопоставление баз данных американских госслужащих с также взломанными базами данных сайта тайных знакомств Ashley Madison, разных финансовых и транспортных компаний и т.д.

Ссылаюсь на доклад американской организации Mandiant (ныне FireEye), автор отдает пальму первенства китайской хакерской группе APT1 (в миру - в/ч 61398, г. Шанхай), в то же время в самом докладе приводится ряд китайских компьютерных атак, которые не удалось связать именно с APT1 [4].

Отмечая технологичность кибератак со стороны китайских киберразведчиков, автор иронически ставит знак равенства между понятиями Advanced Persistent Threat (целевые технологические итерационные атаки, APT) и Asia-Pacific Threat (рис.5).

Не стоит думать, что китайскому хактивизму (Chinese Cyber Horde - по изречению автора) чужды коллективные политические акции, возьмем хотя бы DDOS-атаки на американские сайты во время агрессии НАТО в Европе [1, с.112].

В заключение подраздела хотелось бы напомнить читателям о высоком уровне безопасности киберпространства Поднебесной: цензуре интернет-контента и институте кибертроллей, выделенном интернет-сегменте (Golden Shield Project / Great FireWall of China) и возможности отключения от внешнего кибермира в случае полномасштабной войны, развития средств кибервойны (Great Canon of China), а также об импортоограничении. В последнем случае любознательному читателю будет интересно дополнительно ознакомиться с китайским антитеррористическим законом, вступившим в силу с 1 января 2016 г.

Кибертеатр военных действий США

Стремление к доминированию США в глобальном киберпространстве сопровождается жесткой позицией служб силового блока США и решительной поддержкой их со стороны высшего политического руководства страны.

Несмотря на позицию правозащитников (оппозиции в лице республиканцев), руководство DoD NSA последовательно отстаивает свои интересы, а именно: законодательно фиксирует возможность государства (читай, военного ведомства) вмешиваться в деятельность коммерческих компаний-разработчиков, телекоммуникационных компаний и сервисных интернет-компаний, возможность скрытия информации об уязвимостях в ИТ-продуктах и сервисах, добивается выделения необходимого бюджета, подбора персонала (склонения хакеров к сотрудничеству), проведения киберучений, реформирования и усиления военных киберструктур, наконец, совмещение должности командующего кибернетическим командованием США (US Cyber Command, USCYBERCOM) и директора NSA, при этом, последние являются военнослужащими (никаких гражданских). Вызывает интерес публичность и техническая компетентность

2 www.golos-ameriki.ru/content/chinese-hackers/2913838.html

директора NSA, который успевает лично подискутировать с недостаточно этичными хакерами на самых авторитетных международных хакерских конференциях, как: Black Hat и Def Con.

Автор книги описывает правовой базис USCYBERCOM, основываясь на легендарной «наступательной» директиве верховного главнокомандующего вооруженных сил США - PDD-20 (Presidential Policy Directive 20), которая обозначила роль ведения войны в киберпространстве как и «на суше, воздухе, море и космосе». При этом выделены три миссии USCYBERCOM:

- защита информации в АСУ войсками и силами;
- обеспечение информационной поддержки войск (в сетецентрической войне);
- проведение кибероперацій по нападению и обороне в национальных интересах США.

Несмотря на однозначно определенную роль военных в жизни американцев, автор бестселлера уделяет внимание и другим ведомствами и службам, которые играют важные роли в обеспечении безопасности киберпространства в интересах США, например, Министерству внутренней безопасности (Department of Homeland Security, DHS), Центральному разведывательному управлению (Central Intelligence Agency, CIA), Федеральному бюро расследований (Federal Bureau of Investigation, FBI) (рис.6). Особо автор восхищается следующими подразделениями безопасности киберпространства:

- Tailored Access Operations (TAO) и Remote Operations Center (ROC) из состава DoD NSA,
- Information Operation Center (IOC) из состава CIA,
- Data Intercept Technology Unit (DITU) из FBI.

В то же время, автор по каким-то причинам абсолютно ничего не сказал про построенный в 2013 г. датацентр NSA - Utah Data Center (объем обрабатываемых данных - 5 zettabyte), играющий главную роль в реализации стратегии мирового кибергосподства.

Нет смысла далее пересказывать все содержание произведения, но отметим некоторые ключевые моменты.

Целенаправленные вредоносные программы

Как известно, новая эра киберпротивоборства началась с освещения в прессе нового класса кибероружия - целенаправленной вредоносной программы (ЦВП) Stuxnet в 2010 г. Однако автор приводит пример другой подобной программы (кстати, также распространяющейся через USB-устройства), ставшей достоянием известности годом ранее - Agent.btz (негодуя, что очистка ведомственных компьютеров от Agent.btz заняла 14 месяцев) [1, с.231].

Всего в книги рассмотрены четыре ЦВП: Agent.btz, Aurora, Stuxnet (операция США Olympic Games) и Hacking team RCS. Причину, почему автор проигнорировал хорошо освещенные в печати кибер-скандалы с другими ЦВП (даже не упомянуты линейки Duqu, Flame, Gauss, Wiper), можно искать в его гражданской принадлежности. Впрочем, с остальными ЦВП читатель может самостоятельно ознакомиться, например, на сайте Kaspersky Lab[3].

Справедливости ради следует сказать, что автор приводит много примеров программ класса malware и spyware.

Роль уязвимостей

Напомним, что современные компьютерные атаки основаны на эксплуатации известных (но не

3 https://apt.securelist.com/

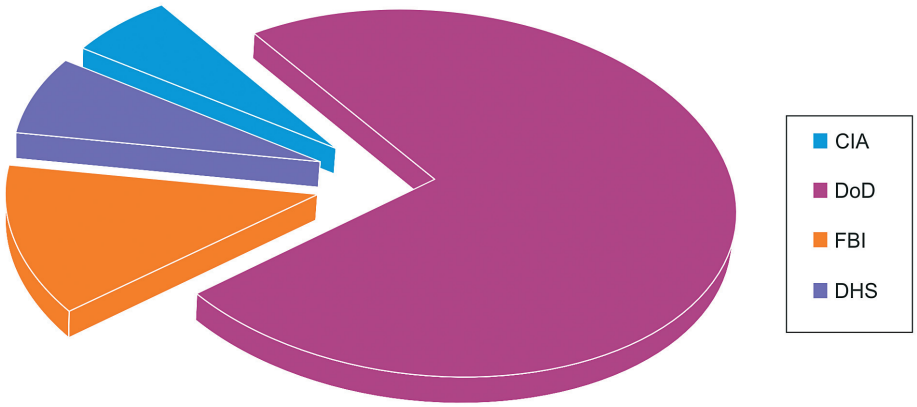


Рис.6. *Публичная активность киберслужб США*

закрытых) уязвимостей и неопубликованных (нулевого дня, zero day) уязвимостей. При этом противоборствующие стороны озабочены:

- выявлением уязвимостей в программном коде;

- приобретением уязвимостей у хакерного сообщества;

- внедрением уязвимостей (закладок, бэкдоров и т.д.) в исходный код;

- внедрением уязвимостей (имплантат) в технические комплексы на этапе поставки и эксплуатации.

Понятно, что победа в кибервойне во многом определяется наличием информации об уязвимостях нулевого дня. Как известно, ЦВП Stuxnet использовал 12 уязвимостей, 4 из которых были известны на момент вторжения [5]. Автор книги рассказывает, что NSA, якобы, имеет базу уязвимостей нулевого дня и их эксплойтов объемом в две тысячи [1, с.159].

В книге приводится пример, что стоимость эксплоита критической уязвимости нулевого дня составляет 50 000-100 000 $, хотя бывают исключения - до 1млн. $. В 2013 году называется бюджет NSA в 25 млн.$ именно на покупку критических уязвимостей нулевого дня. Если учесть, что мега ЦВП разведывательной направленности Flame использовала 3 уязвимости нулевого дня, то легко посчитать, что за 2013 г. NSA имела возможность подготовить до 166 оригинальных ЦВП типа Flame.

Автор повествует как про криминальный онлайн-рынок через Tor (Silk Road – до 2013 г.), так и про легитимный. Например, указывается, что фирма Endgame за 2.5 млн. $ предлагает годовой подписной пакет, в который входит 25 эксплойтов 0-дня. За 1.5 млн $ - доступ к БД, в которой хранится информация о зараженных компьютерах [1, с.169]. Книга не обошла вниманием и NSA-криптозакладки, например, ссылаясь на авторитетное мнение Б.Шнайера [1, с.150].

Между прочим, в 2013 г. мир был шокирован публикацией журналом Spiegel каталога имплантатов NSA (TAO ANTD) [6, 7] - весьма странно, что автор про этот конкретный случай умолчал.

Обвинения и скандалы

Можно выделить три класса обвинений ИТ-фирм в сотрудничестве со спецслужбами, на которых автор заостряет внимание:

1) предоставление спецслужбам онлайн-доступа к информации о клиентах;

2) установка и скрытие от клиентов уязвимостей и недекларированных «полицейских» возможностей в ИТ-продуктах и сервисах;

3) активное участие в кибервойнах.

В плане мониторинга информации о клиентах в книге расписан ряд правительственных разведывательных и контрразведывательных программ и систем:

- Carnivore - система прослушки интернет-трафика (у интернет-провайдеров);

- Stellar Wind - госпрограмма перехвата сообщений электронной почты, телефонных разговоров, финансовых операций и интернет-активностей путем сотрудничества с телекоммуникационными компаниями (называются AT&T, Verizon и т.д.);

- Prism - госпрограмма, в рамках которой спецслужбы США имеют полный доступ к серверам глобальных информационно-коммуникационных компаний, таких как: Microsoft, Google, Yahoo, Facebook, YouTube, Apple и др. Стоит посетовать, что, оценивая глобальную информационную интеграцию таких ИТ-гигантов как Microsoft, Google и Apple в мировую информационную инфраструктуру, можно оценить масштабы бедствия для неамериканских сегментов.

Обвинения в сокрытии и встраивании бэкдоров и других полицейских возможностей сводят на нет какое-нибудь доверие к любой американской ИТ-продукции. Автор описывает ситуации с закладками в продукции: RSA, Cisco, Microsoft. В то же время в интернет много сообщений, касающихся подобных обвинений, связанных, например, с корпорациями Google, Hewlett-Packard, Actel, IBM и др. Автор книги сетует на раскаяния компаний IBM, Hewlett-Packard, Cisco и Microsoft, отмечающих падение спроса на свои продукты, например в КНР после разоблачений шпионажа NSA [1, с.338]. К авторским историям, весьма к месту, подошло бы описание шпионского скандала 2015 года о разведпотенциале жестких дисков Western Digital, Seagate Technology, Toshiba, IBM, Micron Technology и Samsung Electronics и др.[4] Автор книги указывает, что ряд компаний давно вышел за рамки пассивных участников кибершпионажа. Например, любопытна наступательная кибероперация Microsoft - Operation b54, когда корпорация захватила контроль над серверами Citadel, обновив данные на пяти миллионах компьютерах ботсети без ведома владельцев [1, с.191]. Обвинения в активном шпионаже корпорации Google давно стали притчей во языцех.

4 www.reuters.com/article/us-usa-cyberspying-idUSKBN0LK1QV20150217

Выводы

На фоне занимательных повествований, касающихся деятельности различных участников информационного противоборства в глобальном киберпространстве, следует указать на озабоченность военно-политического руководства США по достижению военного превосходства. В этом плане хорошо видны следующие тенденции:

- продолжающееся глобальное доминирование на мировом рынке информационных и коммуникационных технологий;

- создание кибервойск, кибероружия (ЦВП и банков эксплоитов уязвимостей нулевого дня), систем контроля информационного пространства, а также проведение наступательных кибероперациий;

- ведение черных (в первую очередь китайских) и белых списков поставщиков;

- проведение инициатив по повышению защищенности информации предприятий промышленности (от головников до всех соисполнителей);

- подготовка высококвалифицированных специалистов (от проведения всеамериканских школьных соревнований до аккредитации университетов по киберпротивоборству).

К достоинству книги следует отнести весьма богатый материал, касающийся перечисления фирм, участвующих в киберакциях, собственно кибероперациий, государственных программ и инициатив в области информационной безопасности, хакерских ассоциаций и конкретных хакеров, вредоносных программ разного класса.

К недостаткам следует отнести лаконичность в описании как конкретных методик, техник и средств, так и разбора инцидентов.

Надо понимать, что уровень достоверности представленной в книге информации также оставляет желать лучшего, так как ставшие достоянием общественности в рамках интервью события и факты, разумеется, являются в свою очередь частью информационной войны.

Библиографические ссылки:

1. Харрис Ш. Кибер войн@. Пятый театр военных действий / Пер. с англ. – М.: Альпина нон-фикшн, 2016. – 390 с.
2. Кларк Р., Нейк Р. Третья мировая война: какой она будет? Высокие технологии на службе милитаризма. СПб.: Питер, 2011. 336 с.
3. Паршин С.А., Горбачев Ю.Е., Кожанов Ю.А. Кибервойны - реальная угроза национальной безопасности? М.: КРАС АНД, 2011. — 96 с.
4. APT1. Exposing One of China's Cyber Espionage Units. Mandiant, 2013. 74 p.
5. Марков А.С., Фадин А.А. Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet // Вопросы кибербезопасности. 2013. № 1 (1). С. 28-36.
6. Клянчин А.И. Каталог закладок АНБ (Spigel). Часть 1. Инфраструктура // Вопросы кибербезопасности. 2014. № 2 (3). С. 60-65.
7. Клянчин А.И. Каталог закладок АНБ (Spigel). Часть 2. Рабочее место оператора // Вопросы кибербезопасности. 2014. № 4 (7). С. 60-68.

References:

1. Shane Harris @War: The Rise of the Military-Internet Complex. Eamon Dolan/Houghton Mifflin Harcourt; First Edition edition (November 11, 2014), 288 p.
2. Richard A. Clarke, Robert Knake. Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins (April 2, 2010), 312 p.
3. Parshin S.A., Gorbachev Yu.E., Kozhanov Yu.A. Kibervoyny - real'naya ugroza natsional'noy bezopasnosti? M.: KRAS AND, 2011, 96 p.
4. APT1. Exposing One of China's Cyber Espionage Units. Mandiant, 2013. 74 p.
5. Markov A.S., Fadin A.A. Organizatsionno-tekhnicheskie problemy zashchity ot tselevykh vredonosnykh programm tipa Stuxnet, Voprosy kiberbezopasnosti, 2013, No 1 (1), pp. 28-36.
6. Klyanchin A.I. Katalog zakladok ANB (Spigel). Chast' 1. Infrastruktura, Voprosy kiberbezopasnosti. 2014, No 2 (3), pp. 60-65.
7. Klyanchin A.I. Katalog zakladok ANB (Spigel). Chast' 2. Rabochee mesto operatora, Voprosy kiberbezopasnosti. 2014, No 4 (7), pp. 60-68.