

Булатова С.Н., Христодуло А.Д. Обзор вредоносного программного обеспечения в современном мире // Академия педагогических идей «Новация». Серия: Студенческий научный вестник. – 2017. – № 05 (май). – АРТ 134-эл. – 0,4 п.л. - URL: <http://akademnova.ru/page/875550>

РУБРИКА: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.491

Булатова Саида Наилевна

студентка 2 курса, факультет информатики и робототехники

Христодуло Анна Дмитриевна

студентка 1 курса, факультет информатики и робототехники

Научный руководитель: Христодуло О.И., д.т.н., профессор

ФГБОУ ВО «Уфимский государственный авиационный

технический университет»

г. Уфа, Российская Федерация

e-mail: o-hristodulo@mail.ru

ОБЗОР ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В СОВРЕМЕННОМ МИРЕ

Аннотация: В статье дан обзор на некоторые вредоносные программы, повлиявшие на киберсобытия государственных масштабов прошедших лет.

Ключевые слова: вредоносное ПО, кибербезопасность, компьютерный вирус.

Bulatova Saida

2nd year student, features of informatics

Khristodulo Anna

1nd year student, features of informatics

Supervisor: Khristodulo O.I, D.Sc., Full Professor
FGBOU VO "Ufa State Aviation Technical University"
Ufa, Russian Federation

THE REVIEW OF THE MALWARE IN MODERN WORLD

Abstract: The article represents the review of some malicious software affected state-level cyber events of the last years.

Keywords: malware, cybersecurity, computer virus.

1 Введение

После череды киберсобытий последних лет не возникает никаких сомнений, что мир всего лишь перешел на новую ступень войны – войны в киберпространстве. Например – в Китае, где блокировка определенных веб-сайтов является стандартной процедурой, три главные поисковые системы оказались полностью заблокированными в 2007 году [1]. Вскоре после этого инцидента, веб-сайты официальных южнокорейских и американских учреждений, а также некоторых банков и СМИ были поражены тремя волнами крупных DoS-атак. В 2010 году вредоносное программное обеспечение (ПО) под названием Stuxnet, целью которого оказалось поражение ядерных установок, было впервые обнаружено в Иране, а в последствии некоторые из его преемников были замечены на Ближнем Востоке [2].

Позднее, частота и серьезность атак стали значительно возрастать (рис. 1). В августе 2012, государственная нефтяная компания Саудовской Аравии претерпела целенаправленную кибератаку на свои электронные средства [3]. В октябре 2012, веб-сайты шести американских банков подверглись крупномасштабной DoS-атаке [4]. А в январе 2013 вредоносное ПО от флэш-накопителя вывело американскую электростанцию из строя на три недели [5].

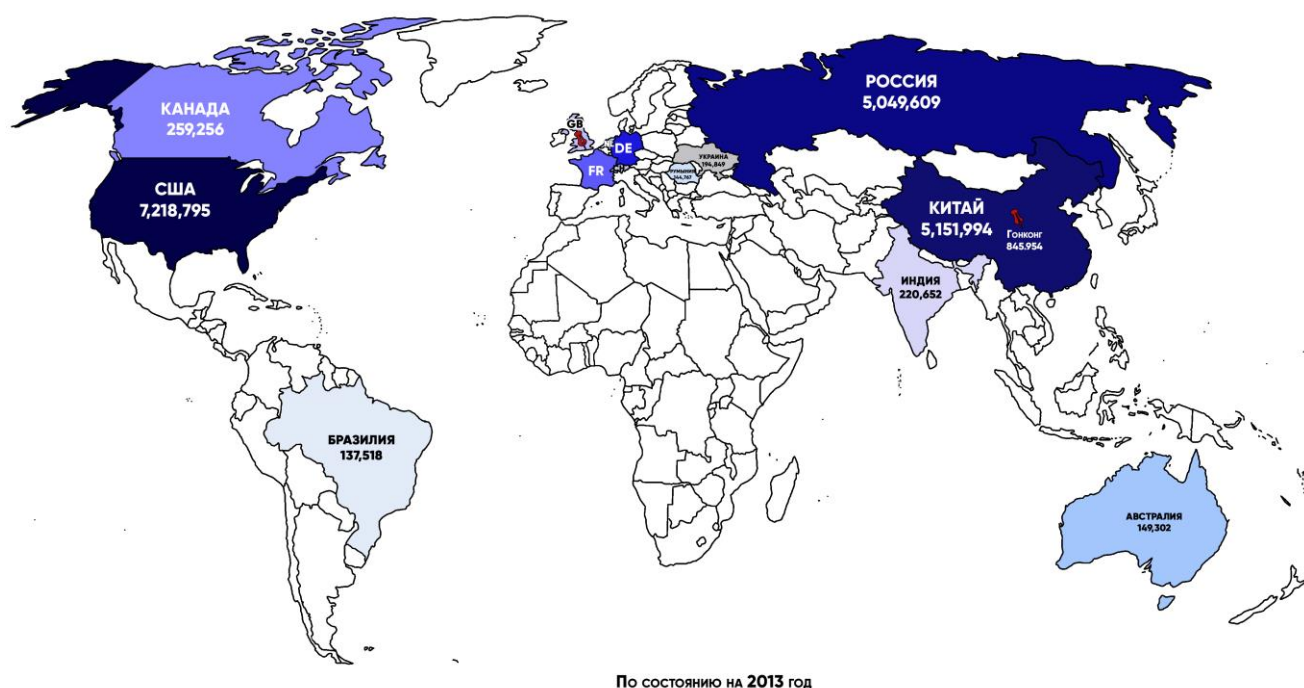


Рисунок 1. Карта, отображающая страны с наибольшей активностью исходящих атак

Обозначение на карте	Страна	Количество атак
DE	Германия	1,689,178
FR	Франция	779,623
GB	Англия	237,392
CH	Швейцария	195,358
NL	Нидерланды	148,690

Таким образом, если возникнет иной глобальный конфликт в текущую эру Западной цивилизации, вполне обоснованно можно заявить, что большая часть этого конфликта будет иметь место быть именно в киберпространстве и вестись с использованием кибероружия.

2. Виды современных вредоносных ПО

В среднем, наибольшая часть всего вредоносного ПО направлена в отношении ИТ-систем, а наиболее популярным на данный момент определенно является так называемая атака “уязвимости нулевого дня”. Хакеры используют атаку “уязвимости нулевого дня”, когда им удастся выявить неизвестное слабое место используемого ПО или операционной системы, которое еще не было выявлено самими разработчиками, или когда не существует готового метода защиты. Пользователи ПО в таком случае находятся в опасном положении ровно до того момента, как поставщики ПО не выпустят доработанную версию ПО, разрешающую данную проблему. Парадокс заключается в том, что в противовес названию этой атаки, обнаружение и исправление этой уязвимости иногда может занимать недели, месяцы и даже годы. Кроме того, хакеры иногда составляют перечень слабых мест, в ряде случаев находящийся в свободном доступе – это означает, что любой пользователь может использовать его для создания вредоносного ПО, на основе конкретной уязвимости выбранной системы.

Стоит отметить также, что сами производители ПО могут внедрить уязвимость нулевого дня во время программирования системы или раскрыть конкретную характеристику уязвимости нулевого дня для различных заинтересованных групп лиц или для государственных организаций – в то время как эти ПО, сделанные по индивидуальному заказу, используются в таких областях, например, как энергетический сектор. Лучшим примером вредоносного ПО, основанного на уязвимости нулевого дня, используемого в качестве оружия государством, а не хакерами-одиночками, является так называемый компьютерный червь “Stuxnet” и его преемники.

Сам Stuxnet был основоположником среди кибернационального оружия – первой частью комплексной группы из нескольких вредоносных ПО, дополняющих друг друга с точки зрения функций и сроков использования, и при этом имеющих единую цель [6]. Слухи о вредоносном ПО Stuxnet появились в среде информационной безопасности впервые в июне 2009, однако реально оно было обнаружено в иранских ядерных установках в 2010 году (**Ошибка! Источник ссылки не найден.**). Самые первые же трассировки “Stuxnet” в ядерных установках Ирана датируются 2005-ым годом.

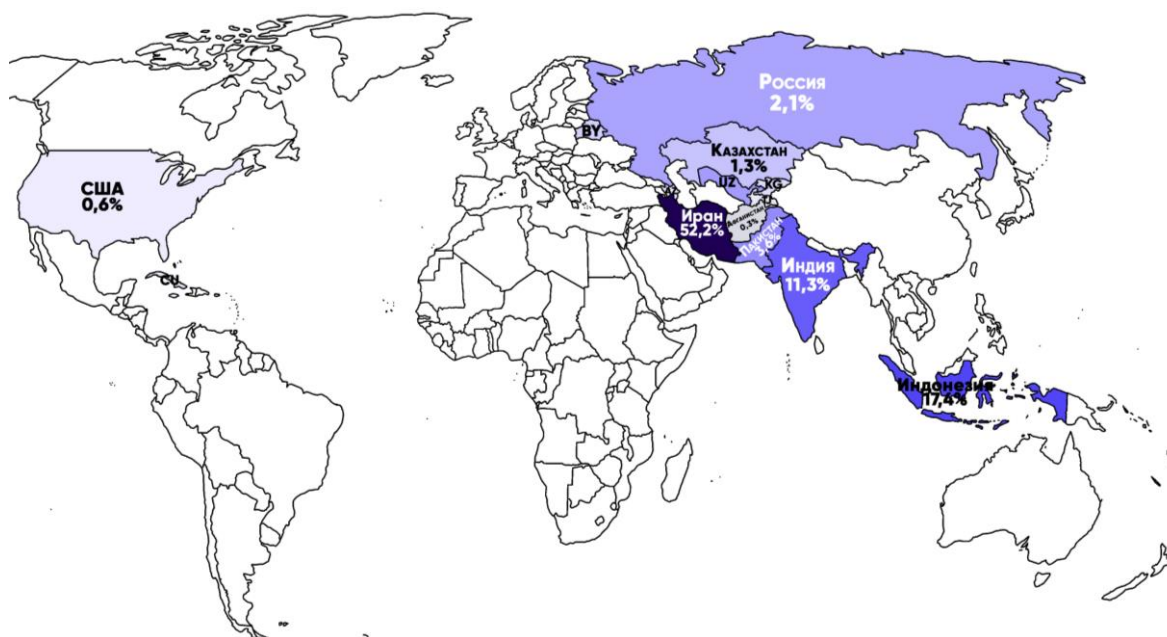


Рисунок 2. Карта, отображающая страны с наибольшим числом зафиксированных инцидентов заражения червем “Stuxnet” (в процентном соотношении)

Обозначение на карте	Страна	Количество атак (%)
UZ	Узбекистан	2,6%
BY	Беларусь	1,1%
KG	Киргизия	1,0%
AZ	Азербайджан	0,7%
CU	Куба	0,6%
TJ	Таджикистан	0,5%

	Другие страны (суммарно)	4,6%
--	--------------------------	------

Проникал этот компьютерный червь главным образом через USB-носители и локальные сети к самой ОС Microsoft Windows, и предназначался исключительно для контроллеров Siemens, что наталкивает на предположение о сотрудничестве между частным ПО или производителями аппаратного оборудования и государством, а именно о том, что “Stuxnet” – это продукт, разработанный совместно спецслужбами США и Израиля.

Как бы то ни было, “Stuxnet” не распространялся посредством крупных источников, атакуя в рамках узкой специализации. Следовательно, чтобы знать, где именно совершать нападения, авторам “Stuxnet”, необходимо было другое вредоносное ПО, которое перед этим собирало бы нужную информацию.

В сентябре 2011, лаборатория “CrySyS” (Лаборатория криптографии и системной безопасности) Будапештского университета технологий и экономики, обнаружила неизвестное троянское шпионящее ПО, работающее главным образом в системах управления производственным процессом на Ближнем Востоке и названное в последствии “DUQU” (

Рисунок 3). Агентство “Symantec” обнаружило, что это шпионское ПО, по всей видимости, произошло от создателей “Stuxnet” [7].

Основная задача “DUQU” состояла в том, чтобы выкрасть цифровые сертификаты, общедоступную и конфиденциальную криптографию, а также проконтролировать и выбрать определенные данные. Позднее, присутствие “DUQU” в Иране [8] было также официально подтверждено иранскими уполномоченными лицами.

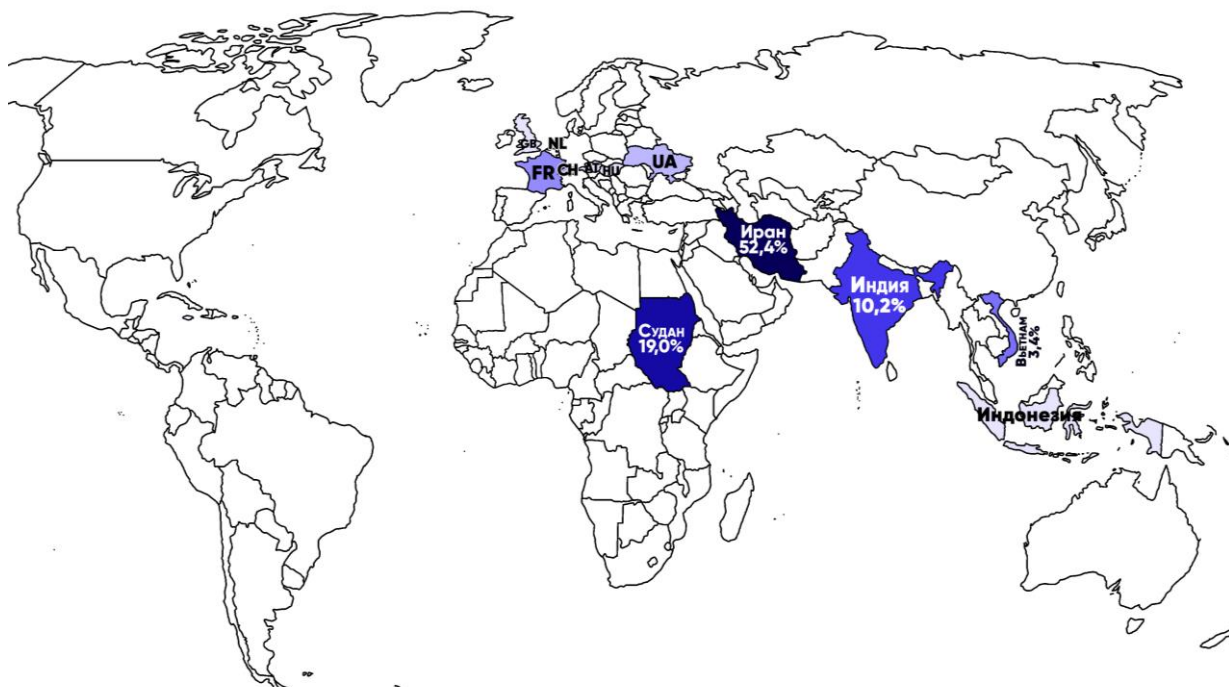


Рисунок 3. Карта, отображающая страны с наибольшим числом зафиксированных инцидентов заражения вирусом “DUQU” (в процентном соотношении).

Обозначение	Страна	Количество атак(%)
FR	Франция	3,6%
UA	Украина	3,3%
CH	Швейцария	3,4%
NL	Нидерланды	2,9%
	Остальные страны (преимущественно Англия(GB), Венгрия(HU), Австрия(AT), Индонезия и др.)	2,8%

В дополнение ко всему, в августе 2012 Лаборатория Касперского обнаружила распространение главным образом на Среднем Востоке трояна [9], который разыскивал конфиденциальную информацию о банковских счетах и финансовых транзакциях пользователей (

Рисунок 4).

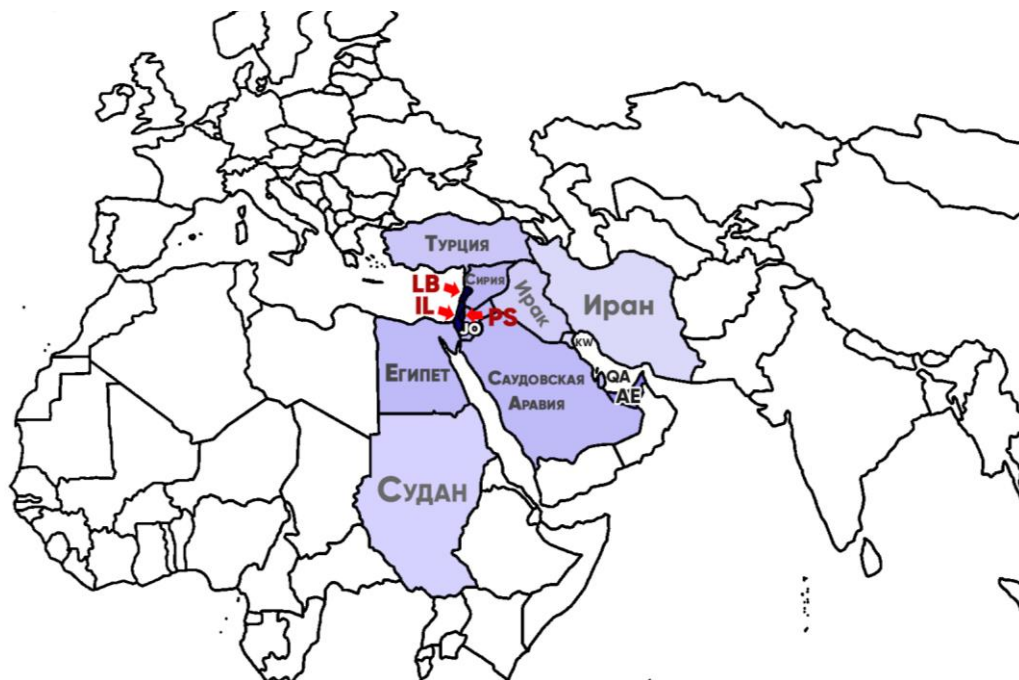


Рисунок 4. Карта, отображающая страны с наибольшим числом зафиксированных инцидентов заражения вирусом “Gauss” (в процентном соотношении).

Обозначение	Страна	Количество атак(%)
LB	Ливан	68,2%
IL	Израиль	19,6%
PS	Палестина	10,7%
AE	ОАЭ	0,5%
	Остальные страны (преимущественно Иордания(ИО), Сирия, Египет, Саудовская Аравия, Катар(QA), Ирак, Турция, Иран, Судан, Кувейт(KW) и др.)	1,0%

Вирус, названный “Gauss”, по всей видимости, создавался некими государственными образованиями, поскольку использовался лишь для отслеживания переводов на выбранном банковском счету.

Несмотря на всё вышеперечисленное, самая большая проблема кибербезопасности обнаружилась в мае 2012 года. Лаборатория Касперского предъявила отчет о существовании самого мощного вредоносного ПО из когда-либо известных, которое было названо “Flame” (Ошибка! Источник ссылки не найден.).

Довольно трудно ответить, каким именно видом вредоносного ПО является “Flame”, поскольку это некая совокупность всего: это и бэкдор, и троянец, и в то же время у него обнаруживаются функции, характерные компьютерному червю, которые позволяют ему тиражироваться в локальной сети и на съемных носителях, если это будет продиктовано его владельцем [10].

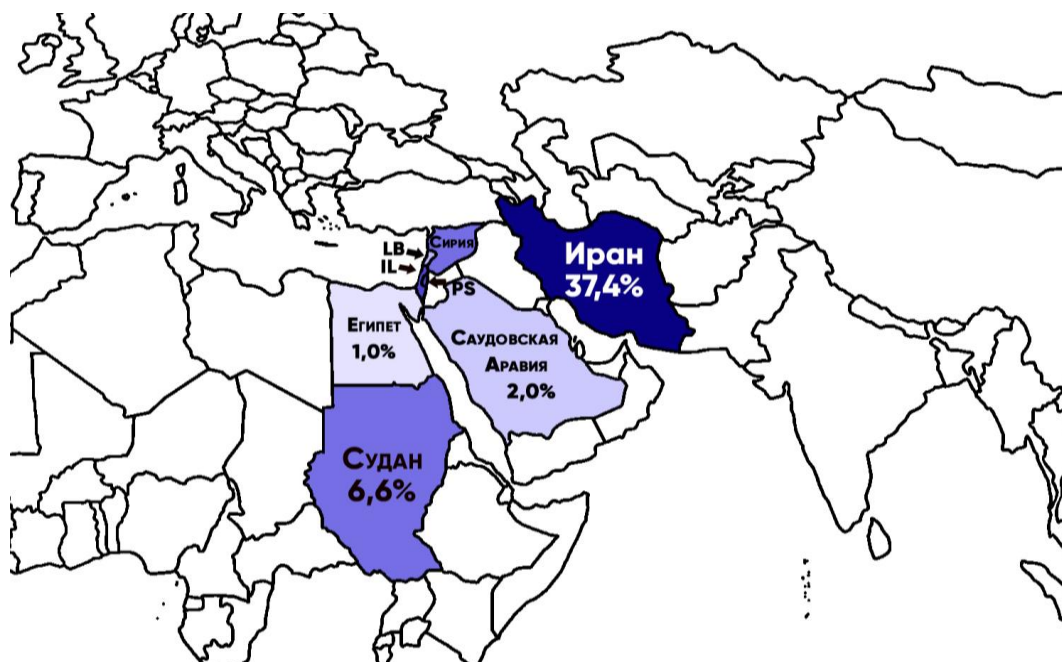


Рисунок 5. Карта, отображающая страны с наибольшим числом зафиксированных инцидентов заражения вирусом “Flame” (в процентном соотношении).

Обозначение на карте	Страна	Количество атак(%)
IL	Израиль	20,4%
PS	Палестина	20,4%
SY	Сирия	6,3%
LB	Ливан	3,8%
	Остальные страны	2,1%

Аналогично своему предшественнику – “Stuxnet”, “Flame” также фокусируется на наблюдении зараженных им ИТ-систем, используя технологию “уязвимости нулевого дня”.

В действительности же, “Flame” может сделать почти все. Помимо обычной записи данных и контроля за процессами, исполняемыми

компьютером, он может также делать снимки экрана исполняемого приложения, производить запись аудиоданных через внутренний микрофон или подсоединиться через Bluetooth-устройство центрального компьютера к другим устройствам и также отслеживать и их действия.

“Flame” не только чрезвычайно большое по размеру вредоносное ПО размером 20 мегабайтов, но также исключительно сложная программа. Он записан частично в форме языка C++, скрипте Lua, а это означает “более трех тысяч строк кода. Примечательно то, что “Flame” – распространялся, по всей вероятности, с марта 2010 – и ко времени, когда Stuxnet был обнаружен, существовал скорее как некий запасной вариант – параллельный альтернативный проект, если какой-либо другой будет распознан и устранен.

Поскольку “Flame” и “Stuxnet/Duqu” работают на разных платформах, но основаны на одном и том же принципе и используют те же методы, представляется вполне возможным, что создатели “Stuxnet” запустили “Flame”, как только “Stuxnet” был публично раскрыт. Однако “Flame”, как широко распространенный вирус, который был зафиксирован даже во французской канцелярии президента, по-видимому, также нуждался в некотором небольшом, более специализированном дополнении.

В июле 2012, Лаборатория Касперского обнаружила “мини-Flame” (“SPE”) – узкоспециализированное вредоносное ПО, распознанное спустя всего несколько десятков случаев заражения. Поскольку “мини-Flame”, как известно, действовало и как часть самого “Flame”, и как часть “Gauss” (и по этой причине использовало его серверы “C&C” совместно с “Flame”), предполагается, что в большинстве случаев “SPE” был установлен серверами “C&C” на системы, которые уже были заражены “Flame” или “Gauss” ранее.

4 Заключение

В войне 21-го века, кибероружие будет определено всё более распространено с точки зрения частоты, а также масштаба использования. Оно является относительно дешевым, в частности для стран с развитым ИТ-сектором, и шанса доказать вину его создателей почти не существует, так как прямые свидетельства взлома системы практически невозможно отследить, а его использование на данный момент не ограничено никакими международными правовыми рамками.

Кроме того, возрастающее число и тяжесть уже произошедших кибератак, которые представлены главным образом семьей вредоносных ПО “Stuxnet” и “Flame”, происхождение которых с наибольшей долей вероятности по всей логике указывает на США – из-за нацеленности на Израиль –являются весомыми причинами для того, чтобы резко разразить кибервойну, особенно в реалиях того мира, где очевидная грубая сила, автор которой известен, неудобна для использования из-за возможности конфликта международных отношений.

В любом случае опасность кибератак от различных субъектов повышается из-за отсутствия четкого международного механизма кибербезопасности (поскольку подавляющее большинство текущих механизмов международной безопасности не покрывает область кибербезопасности).

В завершение хотелось бы отметить, что современный мир подвергся новой смене парадигмы, в которой кибероружие и кибервойна постепенно занимают место обычного оружия и традиционного хода ведения войны. Очевидно, что реальный международный киберконфликт между двумя странами с одинаково высоким развитым ИТ-сектором еще не вспыхнул.

Однако, когда это произойдет, это будет, вероятно, крупномасштабный конфликт с огромными и даже необратимыми последствиями.

Список использованной литературы:

1. <https://lenta.ru/articles/2007/10/19/baidu/>.
2. <http://tass.ru/info/1408961>.
3. <http://www.securitylab.ru/news/428545.php>.
4. https://www.ukrinform.ru/rubric-economix/1399001-hakeri_usilili_kiberataki_na_banki_ssha_1450852.html.
5. <https://www.ridus.ru/news/63219.html>.
6. <http://rus.delfi.lv/techlife/detali/vzломат-celuyu-stranu-virus-stuxnet-okazalsya-chastyu-plana-ssha-po-kibernapadeniyu-na-iran.d?id=47076733>.
7. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf.
8. <https://securelist.com/blog/incidents/32668/the-mystery-of-duqu-part-ten-18>.
9. <https://securelist.ru/blog/spam-test/2930/gauss-gosudarstvennyj-kibershpnionazh-plyus>.
10. <https://securelist.ru/blog/intsidenty/2962/flame-chasto-zadavaemy-e-voprosy>.

Дата поступления в редакцию: 26.05.2017 г.

Опубликовано: 26.05.2017 г.

***© Академия педагогических идей «Новация». Серия «Студенческий научный вестник»,
электронный журнал, 2017***

© Булатова С.Н., Христовуло А.Д., 2017

Всероссийское СМИ

«Академия педагогических идей «НОВАЦИЯ»

Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.

(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru

e-mail: akademnova@mail.ru