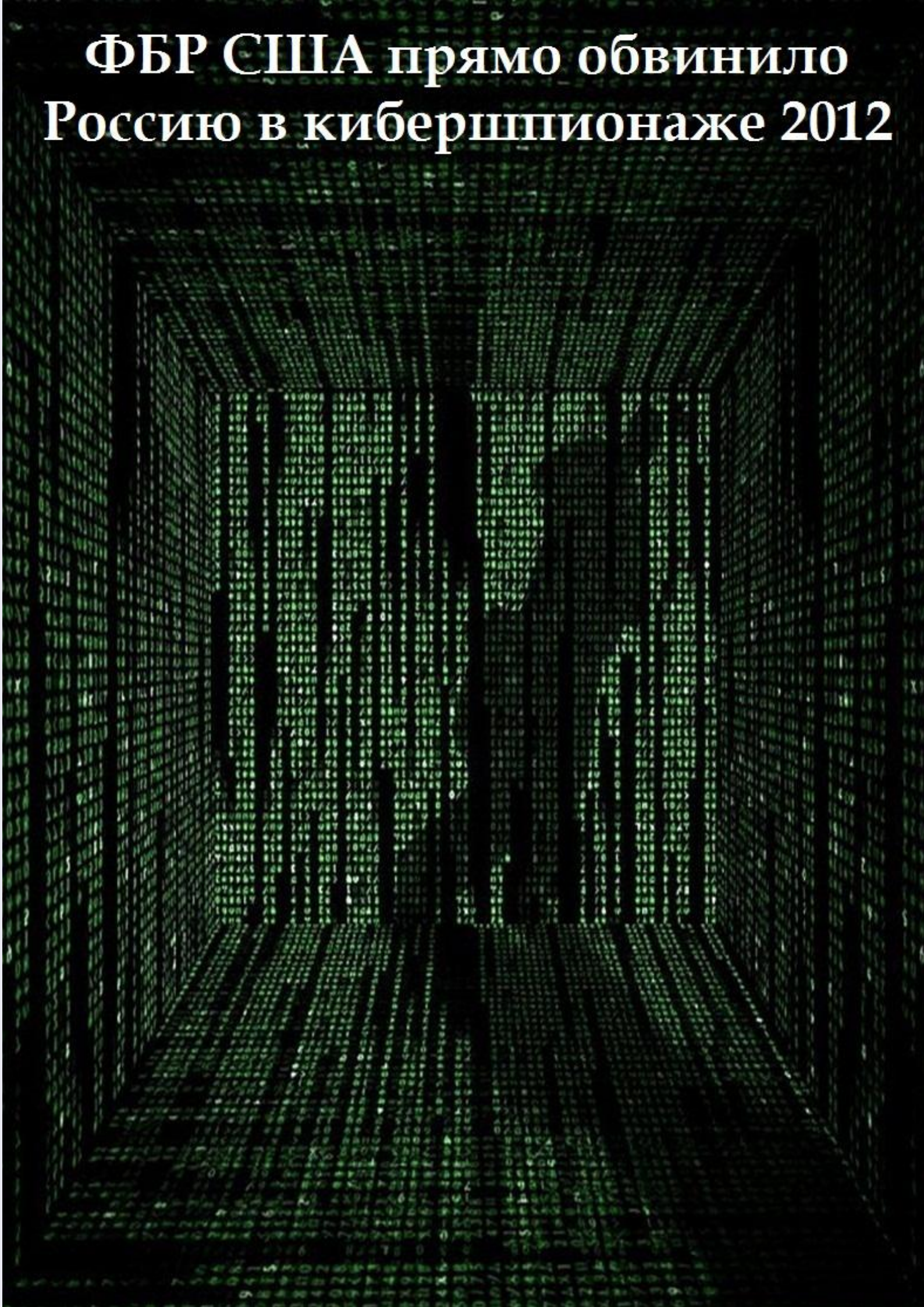
ФБР США прямо обвинило Россию в кибершпионаже 2012



ФБР США прямо обвинило Россию в кибершпионаже 2012.

«Пентагон отныне классифицирует кибератаки со стороны иностранных государств как акт агрессии и предусматривает возможность применения в ответ военной силы», сообщает американская газета ***Wall Street Journal.***

Теперь США считают себя вправе отвечать реальными военными ударами на возможные атаки в киберпространстве. Об этом говорится в новом докладе, который Пентагон подготовил для американского Конгресса. Эксперты назвали этот 12-страничный документ «наиболее чётким заявлением Вашингтона о политике в области кибербезопасности». Смотри в разделе НАТО-ПРО.

Недавно координатор Госдепартамента по вопросам киберпространства Кристофер Пейнтер заявил, что США оставляют за собой право использовать любые средства, в том числе и военные, для отражения кибератак. По его словам, на данный момент самая серьёзная проблема заключается в том, как определить, кто именно стоит за той или иной атакой. Поэтому к военным ударам власти будут прибегать лишь в крайнем случае. Скорее всего, будет война компьютеров. Не зря же президент США Барак Обама подписал план действий в случае сетевой агрессии. В документе определено, в каких случаях военные должны будут просить у президента разрешения на кибератаки вражеских компьютерных сетей. А для этого у американцев есть все возможности.

Кликни !

ФБР США прямо обвинило Россию и Китай в кибершпионаже с целью заполучить секреты США. «Китай и Россия рассматривают себя в качестве стратегических соперников США и наиболее активно занимаются сбором американской экономической и технологической информации, – говорится в докладе под названием «Иностранные шпионы, крадущие экономические секреты США в киберпространстве».

Russian Leaders Link Intelligence Operations and Economic Interests

The SVR "must be able to swiftly and adequately evaluate changes in the international economic situation, understand the consequences for the domestic economy and…more actively protect the economic interests of our companies abroad."
—Vladimir Putin, President, Russian Federation, October 2007

"Intelligence…aims at supporting the process of modernization of our country and creating the optimal conditions for the development of its science and technology."
—Mikhail Fradkov, Director, SVR, December 2010

Source: Russian press reports.

US Partners: Leveraging Access

Certain allies and other countries that enjoy broad access to US Government agencies and the private sector conduct economic espionage to acquire sensitive US information and technologies. Some of these states have advanced cyber capabilities.

Outlook

Because the United States is a leader in the development of new technologies and a central player in global financial and trade networks, foreign attempts to collect US technological and economic information will remain at high levels and continue to threaten US economic security. The nature of these attempts will be shaped by the accelerating evolution of cyberspace, policy choices made by the economic and political rivals of the United States, and broad economic and technological developments.

Near Certainties

Evolving cyber environment. Over the next three to five years, we expect that four broad factors will accelerate the rate of change in information technology and communications technology in ways that are likely to disrupt security procedures and provide new openings for collection of sensitive US economic and technology information. These were identified in studies conducted by Cisco Systems and discussed at the ONCIX conference in November 2010. At the same time, the growing complexity and density of cyberspace will provide more cover for remote cyber intruders and make it even harder than today to establish attribution for these incidents.

The first factor is a *technological shift*. According to a Cisco Systems study, the number of devices such as smartphones and laptops in operation worldwide that can connect to the Internet and other networks is expected to increase from about 12.5 billion in 2010 to 25 billion in 2015. This will cause a proliferation in the number of operating systems and endpoints that malicious actors such as foreign intelligence services or corrupt insiders can exploit to obtain sensitive information. Meanwhile, the underlying hardware and software of information systems will become more complex.

- Marketing and revenue imperatives will continue to lead IT product vendors to release products with less than exhaustive testing, which will also create opportunities for remote exploitation.

An *economic shift* will change the way that corporations, government agencies, and other organizations share storage, computing, network, and application resources. The move to a "cloud computing" paradigm—which is much cheaper for companies than hosting computer services in-

Полный Доклад в разделе НАТО-ПРО.

В нём сообщается, что по-настоящему эффективного противодействия ни американцы, ни британцы организовать кибершпионам не могут. Факт остаётся фактом: можно сколько угодно развивать систему ПРО и наращивать военный контингент, но при этом оставаться незащищёнными от сетевых войн. Причём лишь одна кибератака на секретные информационные массивы может нанести гораздо больший вред, чем деятельность десятков шпионов, работающих старыми методами.

Такое понятие, как кибершпионаж, приобретает особый смысл в свете развития информационных технологий. Сейчас именно Россия и Китай занимают одни из лидирующих позиций по модернизации программного обеспечения, связанного как с распространением вирусного софта, так и с ликвидацией вирусных угроз. Также хорошие программисты есть в Израиле, Индии, Японии… Но больше всего их в американской Силиконовой долине.

Недавно основатель ***Wikileaks*** *Джулиан Ассанж запустил* ***Spy Files*** *– базу данных о разработчиках технологий, с помощью которых спецслужбы следят за владельцами компьютеров и смартфонов. В неё попали две российские фирмы:* ***Oxygen*** *помогает вскрывать мобильники, а* ***ЦРТ*** *– идентифицировать людей по аудиозаписям.*

«Это странно звучит, но сегодня разведки и контрразведки действительно массово используют системы слежения, в том числе за политическими оппонентами, – констатировал Ассанж. – Эта индустрия процветает с 11 сентября 2001 года. Обороты составляют миллиарды долларов в год».

Кликни !

Сейчас в США есть специальные кибервойска, так называемый ***«Сайберком».***

Киберпреступность стоит $ 388 миллиардов долларов ежегодных потерь в глобальном масштабе.

Используемая литература в разделе: http://tvernedra.ru/content/prousa.html

Опубликовано: 12 декабря 2011 года.

http://www.tvernedra.ru/