ОБЩИЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

КИБЕРТЕРРОРИЗМ – УГРОЗА МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

ПШЕНКО КОНСТАНТИН АНДРЕЕВИЧ,
АНИСИМОВ ПЕТР КОНСТАНТИНОВИЧ

АННОТАЦИЯ

В статье рассматриваются особенности кибертерроризма, его разновидности и механизмам действия, а также вопросы по эффективной борьбы с этим принципиально новым видом преступности.

Ключевые слова: глобализация; терроризм; кибертерроризм; хакер; DoS-атака; корневой DNS сервер; wifi; логическая бомба.

CYBER-TERRORISM – THREATS TO INTERNATIONAL SECURITY

PSHENKO K. A.,
ANISIMOV P. K.

ABSTRACT:

The article discusses the features of cyberterrorism, his variety and mechanism of action, and also questions on effectively combat of this fundamentally new type of crime.

Keywords: Globalization; terrorism; cyberterrorism; hackers; DoS-attacks; the root DNS server; Wi-Fi; logic bomb.

В современной мировой политике широко распространено убеждение о том, что глобализация способствует быстрому экономическому развитию. Большему сближению государств и народов в разных областях общественной и политической жизни, и научно-техническому прогрессу. Но, к сожалению, научно-технический прогресс стал прародителем такого явления как кибертерроризм. Само понятие **кибертерроризм** является совокупностью двух слов: кибер, означающее виртуальное пространство, пространство для которого так характерно хранение и перемещение данных, и слово терроризм, которое является международным.

По своей природе Интернет во многих отношениях – идеальное поле деятельности для террористических организаций. Используя сегодня все структуры современного мира от новейшего оружия до интернета, для действия террористов открылось новое поле сражения. Всему этому способствует ряд таких факторов как: "Свободный доступ в сеть из любой точки мира, конфиденциальность, передача информации на больших скоростях на дальние расстояния, создания и поддержания имиджа, пропаганда, легкодоступность в создании собственного веб сайта или аккаунта в социальной сети оставаясь при этом в тени". Это лишь одни из немногих аспектов, которые приводят современное общество к проблеме возникновения кибертерроризма.

Кибертерроризм сегодня является полноценным оружием, так как использует компьютерные системы, программное обеспечение и информационные технологии, разработанные специально для дестабилизации мирового сообщества и ведения террористической деятельности. При этом он не требует больших финансовых вложений, и способен нанести огромный материальный ущерб противнику. Вести отсчет о киберпреступности можно с 70 годов. Так, в 1973 г. кассир нью-йоркского Ситибанка, перевел на свой счет 2 млн. долларов, использовав служебный компьютер, а в 1989 г. американским студентом было заблокировано около 6000 ЭВМ Пентагона, но это было только началом

и по некоторым меркам можно считать детской шалостью [1]. Так как с развитием интернета и всех технологий, сопутствующих ему, трагедии и последствия могут становиться все ужаснее, а идеи и методы все изощрение.

Так, например, А. Дугин в своей работе «Сетевые войны: угроза нового поколения» отмечает, что в сетевой войне чаще всего могут использоваться, как и готовые сети, так и создаваться новые. Наиболее подходящими готовыми сетями являются этнические и религиозные общины. Именно среди этих религиозных сетей и сообществ интернета в целом осуществляется пропаганда и обмен информацией, вербовка новых членов и организация подрывной деятельности. Такой подход, с одной стороны, создает благоприятные условия для рекрутирования все новых террористов, а, с другой, осложняет борьбу с террористическими организациями, которая фактически невозможна в условиях анонимности и общедоступности интернет-коммуникаций. Формирование такого рода сетей порождает проблему обеспечения информационной безопасности, без которой невозможна безопасность международная [2].

На сегодняшний день специалисты по информационной безопасности и борьбе с киберпреступностью разделяют **кибертерроризм на** три уровня [3]:

1. Неструктурированный: использование хаков против информационных систем, обычно используются программы созданные кем-то другим (не самими кибертеррористами). Как правило – самый простой вид атак, потери от него либо минимальны, либо незначительны.
2. Расширенный – **с**труктурированный: возможность вести более сложные атаки против нескольких систем или сетей и, возможно , изменение или создание базовых инструментов взлома. Организация обладает определённой структурой, управлением и прочими функциями полноценных организаций. Также участники таких группировок проводят обучение новоприбывших хакеров.
3. Комплексные – координированные: Способность к скоординированной атаке, способны вызвать массовое нарушение систем безопасности страны. Возможность создания сложных инструментов взлома. Имеют строгую структуру, зачастую представляют собой организации, способные здраво анализировать свои действия, вырабатывать какие-то планы атак и прочее.

На всех трех уровнях используются довольно стандартные методы. Разберем некоторые, наиболее часто применяемые:

– DoS-атаки. Ее задача заключается в том, чтобы компьютер или компьютерная сеть были недоступны пользователю этого компьютера или сети. В пример можно привести одну из самых глобальных в истории DDOS атак от группы *Anonymous.* Она прошла в 2002 году, что привело к выходу из строя 7 корневых DNS-серверов.
– Логические бомбы. Как правило, это алгоритм, задача которого привести к определенным заранее последствиям, которые станут для пользователя неожиданными. Здесь можно привести пример вируса “CHIN” который активизировался 26 апреля 1999 года, в годовщину Чернобыльской аварии. Или пример с АВТОВАЗом ставшим первым предприятием в СССР, на котором в ноябре 1982 года с помощью логической бомбы в компьютерной программе (автор – программист УОП), был остановлен сборочный конвейер.

Третий метод и как показывает практика самый распространенный среди всех – “вирусная атака”. Вирусом называется вредоносное программное обеспечение (ПО), способное проникать в алгоритмы других программ. Так же вирус имеет свойство распространять себя самостоятельно, без непосредственного участия пользователя, чей компьютер заражен. Метод распространения может быть от заражения через Интернет это переход по разного рода ненадежным ссылкам, получения на почту писем с вредоносной программой внутри него до передачи файла по Bluetooth и WiFi-сетям. Хотелось бы отметить, что развитие передачи вирусов через точки доступа по WiFi в современной истории кибертерроризма становится сравнительно новой угрозой. Большинство антивирусов работают по принципу сканирования только устройств хранения, таких как жесткий диск, ОЗУ, USB-носители и сети. В силу такого алгоритма действий антивирус не может определить нахождения на устройстве вредоносной программы.

Этот вирус является серьезной проблемой благодаря легкости распространения сравнимого с гриппом у людей. Таким образом, если зараженное им устройство попадает в места большого скопления компьютеров, к примеру, на фуд-корты, его распространение будет молниеносным в связи с огромным количеством точек доступа. Также его отличительной чертой от других вирусов помимо умения заражать собой девайсы, через WiFi сети является умение задействовать автоматический поиск открытых сетей, при условии попадания им в защищенные паролем сети. Развитие такого рода вирусных программ расширяет спектр действия шпионских организаций, добычи ими информации и новых методов слежения [4]. На ряду с этими уровнями и угрозами существует одно очень важное и стремительно развивающееся благодаря современным IT технологиям направление, которое просто не может оставаться незамеченным с точки зрения проблематики развития кибертерроризма в современном мире. Речь идет о промышленном шпионаже. Его развитие имеет длинную историю в развитых индустриальных государствах, и с развитием новых технологий лица, занимающиеся этим видом шпионажа, получили новые возможности по добычи необходимой информации.

Шпионаж может осуществляться в пользу государства, организации или индивидуального «заказчика». Хотя промышленный шпионаж обычно ассоциируется с частными корпорациями, он может также быть осуществлен против военных сил государства. Например, как установлено Службой безопасности Министерства обороны в докладе 2002 года, важнейшие военные технологии США являются наиболее желанным предметом поиска в мире. Несмотря на то, что пока еще глобальной кибератаки, организованной террористическими группами, не произошло, многие специалисты считают, что террористы достигли того уровня, при котором они могут использовать Интернет (как сам по себе, так и в сочетании с физической атакой) в качестве инструмента для причинения реального вреда.

Многие эксперты говорят о возможности вовлечения в террористические действия хакеров-одиночек и групп хакеров, (далее наемников) не имеющих представления о том, к какому результату могут привести их действия. Стоит сразу пояснить алгоритм их действия. К примеру, проведение хакерской атаки на предприятии, имеющее отношение к оборонной промышленности. А с одного компьтера проведения такого рода операции практически невозможно. Да и не каждый наемник согласится в одиночку взламывать сети предприятий такого рода. Именно поэтому создаются хакерские группировки, а точнее структура, где единым центром управления для координации встает та или иная террористическая организация. Далее создаются подразделения, которые будут находиться под надзором и управлением координирующего центра. В задачи, которого помимо координации действий, входят обязанности подачи дозированной информации. Обладая которой наемники не смогут составить полноценную картину о том, что они делают и на кого работают.

Далее действует очень простая схема – производится удаленная атака на серверные хранилища интересующих их предприятий, похищение информации и отправка письма первым лицам компании с предложением возврата утраченного ими материала за хорошее вознаграждение или иные требования для выполнения выгодные кибертеррористам.

В противном случае информация будет передана их конкурентам. К примеру утрата того или иного скрипта программы или чертежей нового танка будет приравниваться к поражению на информационном поле сражения и провалу всех контр- разведывательных операций. Это пример является лишь одним из немногих вероломных действий террористических группировок, с использованием шантажа и вымогательства денег по средствам использования наемников.

На сегодняшний день для успешного противодействия кибертерроризму необходимо:

- принятие всеобъемлющих законов об электронной безопасности в соответствии с действующими международными стандартами и Конвенциями Совета Европы «О борьбе с киберпреступностью» и «О предупреждении терроризма»;
- организация эффективного сотрудничества с иностранными государствами, их правоохранительными органами и спецслужбами, а также с международными организациями. И наконец, создание национальных подразделений по борьбе с киберпреступностью. Создание международного контактного центра по оказанию помощи для реагирования на транснациональные компьютерные инциденты.

В.В. Путин 9 сентября 2000 г утвердил “Доктрину информационной безопасности” которая представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Настоящая Доктрина служит основой для:

– формирования государственной политики вобластиобеспеченияинформационнойбезопасности Российской Федерации;
– подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
– разработки целевых программ обеспечения информационной безопасности Российской Федерации.
– развития Концепции национальной безопасности Российской Федерации применительно к информационной сфере.

Указом Президента РФ от 15 января 2013 г. на ФСБ России возлагаются полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации компьютерных атак на информационные ресурсы РФ, информационные системы и информационно-телекоммуникационные сети, находящиеся на территории РФ и в дипломатических представительствах и консульских учреждениях РФ за рубежом [5]. В свою очередь, президент США 13 февраля 2013 г. подписал директиву о кибербезопасности, обязывающую создать систему кибербезопасности страны и разработать стандарты и методики, которые помогут снизить риски от кибератак.

В январе 2015 г. государствами-членами ШОС внесены в качестве официального документа ООН «Правила поведения в области обеспечения международной информационной безопасности (МИБ)». Этот документ нацелен на предотвращение конфликтов в информационном пространстве [6].

Таким образом, проблема кибертерроризма является опасной угрозой для международной безопасности, и для борьбы с ним требуются усилия всего мирового сообщества.

Список литературы

1. Повышев В. Борьба с киберприступностью и кибертерроризмом. [Электронный ресурс]. – Режим доступа: http://tmun.utmn.ru/wp-content/uploads/SPChKiber.pdf

2. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбыю [Электронный ресурс]. – Режим доступа: http://www.crime.vl.ru/index.php?p=3626&more=1&c=1&tb=1&pb=1

3. [Электронный ресурс]. – Режим доступа: http://elcomrevue.ru/opredelenie-kiberterrorizma

4. [Электронный ресурс]. – Режим доступа: http://habrahabr.ru/post/215921/

5. Указ Президента РФ от 15.01.2013 N 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/law/review/1685656.html

6. [Электронный ресурс]. – Режим доступа: http://www.mid.ru/brp_4.nsf/0/E4075937EA93964C43257E590068EF82