Секция «Глобальная безопасность»

НАТО и проблема информационной безопасности в современном мире

Научный руководитель – Медовкина Лина Юрьевна

Сильванский Юрий Юрьевич
Студент (бакалавр)
Донецкий национальный университет, Исторический факультет, Кафедра международных отношений и внешней политики, Донецк, Украина
E-mail: mr.hitrojop@mail.ru

Стремительное развитие компьютерных технологий за два последних десятилетия серьезно повлияли на международные отношения. Многие аспекты нашего социума стали сильно зависимы от работы ряда служб и компаний, которые играют далеко не последнюю роль в жизни государств, а что-то и вовсе стало жизненно необходимым. На сегодняшний день очень остро стоит вопрос защиты глобальной безопасности от каких-либо угроз, так как способы взлома и распространения кибертероризма становятся все более изощренее, а способы защиты и решения последующих проблем просто не в состоянии противостоять огромному давлению со стороны агрессора.

Проблематика в обеспечении безопасности в информационном пространстве затрагивает многие аспекты нашего социума. Эксперты из Центра зашиты информационной безопасности НАТО утверждают, что милитаризация интернета является одной из наиболее глобальных и опасных проблем сегодняшнего дня. Современные военные структуры готовы использовать информационное пространство как “поле битвы”. Из этого следует вывод, что крушение безопасности в информационном пространстве влечет серьезные последствия и в реальной жизни, что несомненно усложняет вопрос решения данной проблемы.

Поэтому, НАТО предприняла меры для улучшения безопасности в сфере информационного пространства. В 2008 г. был создан орган по осуществлению защиты в киберпространстве. Основная задача органа заключалась в обеспечении и улучшении безопасности в информационном пространстве, а так же в поиске и решении проблем. Следовательно, в НАТО была создана система специализированных механизмов и институтов оперативного и стратегического назначения для борьбы с падением безопасности в информационном поле.

Всё, чего НАТО так опасалось и готовилось, произошло 12 мая 2017 года. Компьютерный вирус «WannaCry» обрушился на все мировое сообщество и нанес непоправимый урон его аспектам, что кардинально изменило представление и значение понятия кибертерраризма. Вскоре, после глобальной кибератаки 12 мая стало известно, что в ходе крупной кибератаки пострадали больницы Великобритании, а вечером этого же дня, глава антивирусной компании Avast Якуб Кроустек заявил, что вирус атаковал и зашифровал свыше 55 тысяч компьютеров. Позже, российская Лаборатория Касперского установила более 47 тысяч атак кибервирусом WannaCry в 76 странах мира. Том Боссерт, советник президента безопасности США подтвердил, что 15 мая был осуществлен взлом свыше 280 тысяч компьютеров в 150 странах мира [3].

По оценкам экспертов, только за первые четыре дня крупномасштабной атаки вирусом WannaCry пострадали более 300 тысяч пользователей в 150 странах мира. Суммарная оценка ущерба составляет сумму 1 млрд долларов США и утраты продолжают расти.

Что является не маловажным, в общую оценку ущерба вошли потеря данных, снижение производительности, простои в работе, судебные издержки, репутационные ущербы и другие факторы. Хочется отметить, что данная накопленная сумма образовалась в течении нескольких дней, а специалисты в области антивирусного обеспечения и по сей день не смогли полностью приостановить распространение вируса.

Вирус является главным аспектом кибератаки, именно червь-шантажист, именуемый WannaCry. В ходе атаки и последующего заражения компьютера вирус-червь быстро распространяется по всей локальной сети, в которой производит шифрование файлов, а позже предлагает выплатить определенную сумму за разблокировку интернет-валютой (Bitcoin). Было отмечено, что вирус использует средства и инструменты, которые киберпреступники украли у хакеров из АНБ США еще в 2000-х годах.

Особое внимание стоит уделить тому факту, что высокая частота кибератаки вирусом WannaCry была установленна в таких странах как: Великобритания, Германия, Россия, Украина, Италия, Турция, Испания, Португалия, Япония, Тайвань. Серьезнейший урон получили Германия, США и Великобритания. Также следует отметить, что атаке вируса WannaCry подверглись:

- больницы Великобритании. Огромное количество больниц осталось без каких-либо средств коммуникации, а пациенты, которые остро нуждались в медицинской помощи оказались тяжелейшем положении.

- железнодорожный оператор Германии Deutsche Bahn. В Ганновере были атакованы и заблокированы все диспетчерские системы управления. Вирус имел все возможности повлиять на режимы и графики движения поездов Deutsche Bahn.

- 15 мая представитель МНБ США заявил, что во время кибератаки было осуществлено заражение компьютеров операторов объектов инфраструктуры США [2].

Анализируя изложенное следует отметить, что каждая инфраструктура играет важную роль в работе основных служб и производственных систем в нашем современном обществе, что несомненно влияет на жизнь любого человека. Поэтому сбои, блокировка, ограничения или какие-либо неполадки в сферах информационной безопасности могут иметь необратимые последствия для нашего социума, что может привести к нарушению установленного порядка, влиянию органов правления, а экономика и гос-безопасность и вовсе могут рухнуть за считанные часы.

Источники и литература

1) Киселёв В. Костенко А. Кибервойна, как основа гибридной операции (рус.) // Армейский сборник: журнал. — 2015. — Ноябрь (т. 257, № 11). — С. 3-6.

2) Об атаке вируса Wannacry // «ФинЦЕРТ» Банка России 2017 г.

3) Сошников, Андрей. WannaCry: как работает крупнейшее компьютерное вымогательство. «Русская служба Би-би-си» 2017 г.

4) Шариков, П. А. Информационный комп- лекс / П. А. Шариков // Безопасность Европы / Ин-т Европы РАН. – М. : Весь мир, 2011. – С. 581–591.

5) Geers, K. Strategic Cyber Security / K. Geers. – NATO Cooperative Cyber Defence Centre of Excellence, 2011. – 169 p.