Столыпинский
вестник

Научная статья
Original article
УДК 004.056

КИБЕРТОРРОРИЗМ-ЗНАЧИТЕЛЬНАЯ УГРОЗА КИБЕРБЕЗОПАСНОСТИ

CYBERTORRORISM IS A SIGNIFICANT CYBER SECURITY THREAT

Смирнов Виталий Михайлович, к.т.н., старший преподаватель кафедры информатики и математики Московского университета МВД имени В.Я. Кикотя. (Россия 117997, г. Москва, ул. Академика Волгина, д. 12.), тел. 8(926) 36-74-76

Иванова Карина Зуфаровна, курсант Московского университета МВД имени В.Я. Кикотя. (Россия 117997, г. Москва, ул. Академика Волгина, д. 12), тел. 8(951) 210-34-72,lady.karina75@mail.ru

Smirnov Vitaly Mikhailovich, Candidate of Technical Sciences, Senior Lecturer at the Department of Computer Science and Mathematics of the Moscow University of the Ministry of Internal Affairs named after V.Ya. Kikot. (12 Akademika Volgina str., Moscow, 117997, Russia), **tel.** 8(926) 36-74-76

Ivanova Karina Zufarovna, cadet of the V.Ya. Kikot Moscow University of the Ministry of Internal Affairs. (12 Akademika Volgina str., Moscow, 117997, Russia), **tel.** 8(951) 210-34-72, lady.karina75@mail.ru

Аннотация: В статье рассматривается такая глобальная проблема как кибертеррризм. Данное преступление достаточно широко распространено во всем мире благодаря цифровизации всего общества.

Abstract: This article deals with such a global problem as cyberterrorism. This crime is quite widespread throughout the world due to the digitalization of the entire society.

Ключевые слова: Кибертерроризм, цифровизация, государство, общество, информация.

Keywords: Cyberterrorism, digitalization, state, society, information.

В мире стремительно растет количество устройств интернета, с помощью которых преступные организации и мошенники намеренно атакуют сети Интернета с целью террора или шантажа. В настоящее время Интернет является широкомасштабной сетью, которой пользуются большинство людей в мире. С развитием новых информационных технологий рождаются новые угрозы, с которыми усиленно борются государственные органы в области информационной безопасности. Термин «кибертерроризм» употребляется довольно часто как в СМИ, так и в юридической литературе, но каждый автор находит новые слова для данного термина. Кибертерроризмом принято считать акты, которые совершенны одним человеком или группой людей, с целью влияние на экономические, политические и внутригосударственные отношения.

Так же кибертерроризм представляет собой правонарушение, совершаемые в компьютерной среде, либов сети Интернет.

Кибертерроризм не является примитивным видом терроризма. В данном виде не закладываются бомбы, не берут заложников. Все происходит не в реальном пространстве, а виртуальном мире. Кибертерроризм опасен выводом из строя масштабной компьютерной сети влиятельной компании, уничтожением данных клиентов банков, нарушением работы крупных компаний и предприятий, с целью захвата и уничтожения определенной секретной информации, либо получения за эту информацию выкупа.

Кибертеррористы угрожают компьютерными средствами Участников террористических группировок можно встретить на разных форумах и в

чатах, также они имеют свои собственные сайты. Социальные сети и другие подобные ресурсы, которые используются для вербовки новых участников запрещенными группировками. Для достижения поставленных целей они могут использовать различные методы, а именно:

-Незаконное получение доступа к государственным и военным архивам с секретной информацией, реквизитам банковских счетов и платежных систем, личным данным;

-Осуществление контроля над объектами инфраструктуры для оказания влияния на их работоспособность вплоть до вывода из строя отдельных компонентов и полной остановки систем жизнеобеспечения;

-Похищение или уничтожение информации, программных средств или технических ресурсов путем внедрения вредоносного ПО различных типов;

-Ложные угрозы совершения атак, которые могут повлечь за собой дестабилизацию экономической или социально-политической обстановки.

В большей степени развитию кибертерроризма влияет тотальная цифровизация человеческого общества. К ним можно отнести использование различных аппаратных и программных средств, например,

-Троянские программы или компьютерные вирусы, которые предназначены для предоставления различной информации из удаленных сетей;

-Специализированные компьютерные вычислительные станции, предназначенные для совершения кибер-атак на различные информационные сервисы и ресурсы с их последующим выводом из строя;

-Иные виды информационного оружия и средств.

В Указе Президента Российской Федерации от 31.12.2015 N 683 «О Стратегии национальной безопасности Российской Федерации» отмечено, что «…появляются новые формы противоправной деятельности, в частности с использованием информационных, коммуникационных и высоких

технологий»[1]. Первоначальным фактором появления кибертерроризма является цифровизация и компьютеризация человечества и общества в целом. Кибертерроримзм отличает от других способов незаконного получения информации тем, что именно в данном методе преступник завладевает информацией при помощи использования различных программных и аппаратных средств, таких как:

1. Троянские программы и модифицированные компьютерные вирусы.
2. Специализированные компьютерные вычислительные станции, при помощи которых совершаются кибер-атаки на сервисы и ресурсы.
3. Иные виды информационного оружия.

Целью кибертерроризма не являются отдельные источники информации граждан, кибертерроризм нацелен на широкие масштабы – кража и уничтожение каналов СМИ, подавление или уничтожение каналов связи и т.д.

Кибертерроризм является достаточно острой проблемой во всем мире. Его жертвой могут стать как простые граждане, так и коммерческие структуры, банковские учреждения, а также не застрахованы от данной угрозы органы государственной власти. Для борьбы с данной проблемой все государства мира объединяют свои силы. В борьбе с кибертерроризмом занимаются различные международные организации как Организация Объединенных Наций, Совет Европы, Интерпол, Международная организация экспертов и прочие. Ведущая роль отдается ООН, а именно ее главным органом – Совету Безопасности, Генеральной Ассамблее и различным неформальных партнерствам.

В 2001 году была принята специальная Конвенция «О киберпреступности», в которой были определены преступления, совершаемые в информационной среде и относимые к категории киберпреступлений.

---

[1] Указ Президента РФ от 31.12.2015 N 683 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс] URL: https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html(дата обращения: 24.05.2021).

[2] По условиям данной Конвенции все государства должны были создать условия, которые позволили бы компетентным органам в борьбе с кибертерроризмом пресекать преступления в сфере Интернета и восстанавливать нарушенные права граждан.

В наше время положений Конвенции недостаточно для успешной борьбы с кибертерроризмом. И поэтому сейчас большинство стран мира разрабатывают различные законодательные акты, которые необходимы для борьбы со стремительно развивающейся проблемой в мире.

Зависимость от Интернета растет с каждым днем с геометрической прогрессии. Для террористов кибер-атаки являются преимущественным методом совершения преступлений, по сравнению с физическими атаками. Благодаря высокому уровню развития техники террорист может нанести больший вред, чем взрывные устройства, посредством подключенного к интернету компьютера. Совершать акты компьютерного террора способны многие организации экстремистской направленности: ИГИЛ, Аль-Каида, ИРА,различные религиозные движения и прочие незаконные вооруженные формирования.

Учитывая все изложенное, можно выделить ряд позиций, которые направлены на совершенствование противодействия кибертерроризму:

• разработка государственной стратегии предупреждения кибертерроризма в современном российском обществе должна включать в себя не только карательно-восстановительные, но и превентивно-профилактические меры, основанные на информационном воздействии и противодействии причинам и условиям, инициирующим развитие экстремистской деятельности в сети Интернет;

• закрепление в законодательстве понятия «кибертерроризм»;

• создание институтов специальной нормативной и общественной экспертизы материалов экстремистского и террористического содержания в сети Интернет;

[2] https://spravochnick.ru/mezhdunarodnye_otnosheniya/kiberterrorizm_kak_novaya_globalnaya_ugroza/

• создание антитеррористического информационного «фронта» в целях обнаружения угроз безопасности путем создания единых систем и банков данных, в которых будут фиксироваться террористические организации, используемые ими информационные каналы.

Следует не забывать-большая вероятность, что кибер-атак в будущем будет намного больше, сфера информационных технологий развивается быстрее, чем законодательство. Всё это усложняет борьбу с кибертерроризмом, поэтому уже сейчас нужно задумываться о надежной защите информации не только граждан, но и целых государств.

Литература

1. Указ Президента РФ от 31.12.2015 N 683 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс] URL: https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html(дата обращения: 24.05.2021).
2. https://spravochnick.ru/mezhdunarodnye_otnosheniya/kiberterrorizm_kak_novaya_globalnaya_ugroza/

References

1. Decree of the President of the Russian Federation of December 31, 2015 N 683 “On the National Security Strategy of the Russian Federation” [Electronic resource] URL: https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html (date accessed: 05/24/2021).
2. https://spravochnick.ru/mezhdunarodnye_otnosheniya/kiberterrorizm_kak_novaya_globalnaya_ugroza/

Для цитирования: Иванова К.З. КИБЕРТОРРОРИЗМ-ЗНАЧИТЕЛЬНАЯ УГРОЗА КИБЕРБЕЗОПАСНОСТИ//Научный сетевой журнал «Столыпинский вестник» №4/2022