НАУЧНАЯ АРТЕЛЬ
АКАДЕМИЧЕСКОЕ ИЗДАТЕЛЬСТВО

16+

ISSN (p) 2712-9497
ISSN (e) 2542-1034

№ 3/2023

НАУЧНЫЙ ЖУРНАЛ
«EO IPSO»

Москва
2023

Гылышаев Мейлис,
магистрант
Институт международных отношений
Министерства иностранных дел Туркменистана.
Ашхабад, Туркменистан.

МЕЖДУНАРОДНО ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Аннотация

В последние годы кибербезопасность, то есть безопасность компьютеров, компьютерных сетей и систем, управляемых компьютером, стала главной темой международной политики. Многие страны, региональные союзы стран и международные организации создали стратегии кибербезопасности, а также группы реагирования на инциденты кибербезопасности.

Ключевые слова:

Кибербезопасность, киберугрозы, Международные подходы обеспечения кибербезопасности, функции безопасности.

Annotation

In recent years, cybersecurity, that is, the security of computers, computer networks and computer-controlled systems, has become the main topic of international politics. Many countries, regional alliances of countries, and international organizations have established cybersecurity strategies as well as cybersecurity incident response teams.

Key words:

Cyber security, cyber threats, International approaches to cyber security, security functions.

Международный союз электросвязи (МСЭ) ведет репозиторий таких документов по стратегии кибербезопасности [1], но обычно они также доступны на веб-сайтах соответствующих правительств и организаций. Несколько международных конвенций о киберпреступности были подписаны разными группами стран [3; 4; 5; 6]. Существуют большие различия между стратегиями и целями, опубликованными разными странами и организациями. Одни занимаются только кибершпионажем и кибервойнами, другие охватывают весь спектр кибербезопасности от защиты от потери данных или разрушения критической информационной инфраструктуры в результате стихийных бедствий или человеческих ошибок, а также защиты данных и конфиденциальности [7] и кибервойн.

Описанные угрозы варьируются от чисто информационных технологий до потенциальных атак на критическую инфраструктуру и промышленные системы.

Исторически угрозы кибербезопасности начинались с потери данных из-за простых человеческих ошибок или системных сбоев на отдельных компьютерах. С изобретением компьютерных коммуникационных сетей возникли ошибки при передаче данных, что открыло возможность отправки данных получателям, не уполномоченным на получение данных. Мы должны иметь в виду, что первые компьютерные сети соединяли научные организации, которые хотели обмениваться некоммерческими данными – сначала посредством обмена по электронной почте, а затем с появлением Всемирной паутины (WWW) [8]. Коммерческие приложения WWW последовали позже. Следовательно, первые протоколы обмена данными между компьютерами разрабатывались

без учета безопасности данных. Также операционные системы, используемые на компьютерах, не были предназначены для защиты от вторжений извне. Все функции безопасности — брандмауэры, антивирусные сканеры и т. д. — являются надстройками и исправлениями для системы, которая изначально пренебрегала безопасностью данных, поскольку исходные данные не нуждались в защите. Добавление функций безопасности произошло в то время, когда размеры существующих операционных систем и протоколов связи были уже достаточно большими и содержали множество уязвимостей, позволяющих проникнуть в систему. Но даже сегодня в новом программном обеспечении создается много новых уязвимостей из-за пренебрежения безопасными процедурами создания программного обеспечения.

Давайте сначала рассмотрим чистые угрозы информационной безопасности, а затем дополнительные угрозы, связанные с сочетанием информационных технологий (ИТ) и операционных технологий (ОТ). Как упоминалось выше, первыми угрозами кибербезопасности были человеческие ошибки или непреднамеренный сбой системы. Основным решением было хранение копий данных либо локально, либо в удаленном месте для защиты от стихийных бедствий. С появлением WWW удаленное копирование данных через Интернет в одно или несколько отдельных мест стало обычной мерой для крупных организаций. Затем появились хакеры-одиночки, которые либо просто хотели показать, что могут взломать системы, к которым у них не было легального доступа, либо хотели украсть данные для личной эксплуатации. Некоторые также хотели помешать использованию определенных систем с помощью, так называемых атак типа «отказ в обслуживании» (DoS). Чтобы понять атаки и потенциальные контрмеры, мы должны рассмотреть, как эти атаки работают.

Проблема с отслеживанием данных в Интернете заключается в существовании “даркнета” [9]. Можно использовать так называемую луковую маршрутизацию для передачи кода или данных с одного компьютера через цепочку компьютеров к конечному получателю. При использовании этого метода каждый отправитель знает только следующего получателя, но не следующих получателей. Если бы действия всех компьютеров в цепочке были доступны следователям, все равно можно было бы отследить конечного получателя. Но в даркнете для многих компьютеров файлы журналов, отслеживающие все действия на компьютере, могут быть недоступны, или ведение журнала может быть вообще отключено. Особая проблема возникает, когда цепочка пересекает страну, которая считается враждебной или не заслуживающей доверия. Поддержка может быть не предложена или ей нельзя доверять. В этом случае третья сторона может использовать арендованные ботнеты в соответствующей стране для отправки данных через эту страну, а затем в реальный пункт назначения. Тем самым, красиво скрывая свою идентичность и обвиняя в действиях другую страну.

Список использованной литературы:

1. Роль региональных организаций в укреплении доверия в информационном пространстве / The Shanghai Организация сотрудничества, 24 января 2019 г. – Режим доступа: eng.sectsco.org/news/20190124/506016.html.

1. Ott, Nikolas. "Organization for Security and Co-operation in Europe 2019 Chairmanship OSCE-wide cyber/ICT security conference Opening remarks." (2019).

2. Hunting Malware in the Deep Web / Infosec Institute, 10 February 2015. – Access mode: https://resources.infosecinstitute.com/hunting-malware-deep-web.