Научная статья
Original article
УДК 004.424

КИБЕРВОЙНА

CYBERWAR

Казарян Каторина Камоевна студент специалитета, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), kazaryan_katorina@mail.ru

Белан Виктория Вадимовна магистрант, Донской государственный технический университет, г. Ростов-на-Дону, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), viktoriyabelan2018@gmail.com

Kazaryan Katorina Kamoevna specialty student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), kazaryan_katorina@mail.ru

Belan Victoria Vadimovna Master student, Don State Technical University, Rostov-on-Don, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), viktoriyabelan2018@gmail.com

Аннотация: Кибервойна обычно определяется как кибератака или серия атак, направленных на страну. Он может нанести ущерб государственной и гражданской инфраструктуре и нарушить работу важнейших систем, что приведет к ущербу для государства и даже гибели людей.

Однако среди экспертов по кибербезопасности ведутся споры о том, какой вид деятельности представляет собой кибервойну. Министерство обороны США (DoD) признает угрозу национальной безопасности,

исходящую от злонамеренного использования Интернета, но не дает более четкого определения кибервойны. Некоторые считают кибервойну кибератакой, которая может привести к смерти.

Abstract: Cyberwar is usually defined as a cyberattack or a series of attacks aimed at a country. It can damage government and civilian infrastructure and disrupt critical systems, resulting in government damage and even death.

However, there is a debate among cybersecurity experts about what type of activity constitutes cyberwar. The U.S. Department of Defense (DoD) recognizes the threat to national security posed by the malicious use of the Internet, but does not provide a clearer definition of cyberwar. Cyberwar is considered by some to be a cyberattack that can lead to death.

Ключевые слова: Кибервойна, кибератака, DoD, атаки типа отказа в обслуживании

Keywords: Cyberwar, cyberattack, DoD, denial of service attacks

Кибервойна обычно включает в себя кибератаки одного национального государства на другое, но в некоторых случаях атаки осуществляются террористическими организациями или негосударственными субъектами, стремящимися к достижению цели враждебной нации. В новейшей истории есть несколько примеров предполагаемой кибервойны, но не существует универсального формального определения того, как кибератака может представлять собой акт войны.

7 типов атак кибервойны

Вот некоторые из основных типов атак кибервойны.



Шпионаж

Относится к мониторингу других стран с целью кражи секретов. В кибервойне это может включать использование ботнетов или целевых фишинговых атак для компрометации конфиденциальных компьютерных систем до того, как будет украдена конфиденциальная информация .

Саботаж

Правительственные организации должны определить конфиденциальную информацию и риски, если она будет скомпрометирована. Враждебные правительства или террористы могут украсть информацию, уничтожить ее или использовать инсайдерские угрозы, такие как недовольные или неосторожные сотрудники или государственные служащие, связанные с атакующей страной.

Атаки типа отказа в обслуживании (DoS)

DoS-атаки предотвращают доступ законных пользователей к веб-сайту, наводняя его поддельными запросами и заставляя веб-сайт обрабатывать эти запросы. Этот тип атаки может использоваться для нарушения критических операций и систем и блокировки доступа к конфиденциальным веб-сайтам для гражданских лиц, военных и сотрудников служб безопасности или исследовательских организаций.

Электросеть

Атака на энергосистему позволяет злоумышленникам отключить критически важные системы, нарушить работу инфраструктуры и

потенциально нанести телесные повреждения. Атаки на электросеть также могут нарушить связь и сделать такие услуги, как текстовые сообщения и связь, непригодными для использования.

Пропагандистские атаки

Попытки контролировать умы и мысли людей, живущих в целевой стране или сражающихся за нее. Пропаганду можно использовать для разоблачения позорной правды, распространения лжи, чтобы заставить людей потерять доверие к своей стране, или для того, чтобы встать на сторону своих врагов.

Экономический кризис

Большинство современных экономических систем работают с использованием компьютеров. Злоумышленники могут атаковать компьютерные сети экономических учреждений, таких как фондовые рынки, платежные системы и банки, чтобы украсть деньги или заблокировать доступ людей к необходимым им средствам.

Неожиданные атаки

Это киберэквивалент таких атак, как Перл-Харбор и 11 сентября. Смысл в том, чтобы провести массированную атаку, которую противник не ожидает, позволяя атакующему ослабить свою защиту. Это можно сделать, чтобы подготовить почву для физического нападения в контексте гибридной войны.

Примеры операций кибервойны

Вот несколько получивших широкую огласку примеров кибервойны за последнее время.

Stuxnet Вирус

Stuxnet был червем, атаковавшим иранскую ядерную программу. Это одна из самых изощренных кибератак в истории. Вредоносные программы распространяются через зараженные Универсальные устройства последовательной шины и целевой сбор данных и системы диспетчерского управления. Согласно большинству сообщений, атака серьезно подорвала способность Ирана производить ядерное оружие.

Sony Pictures Взлом

Нападение на Sony Pictures последовало за выпуском фильма «Интервью», в котором Ким Чен Ын изображался в негативном свете. Атаку приписывают хакерам из правительства Северной Кореи. ФБР обнаружило сходство с предыдущими атаками вредоносного ПО, совершенными северокорейцами, включая код, алгоритмы шифрования и механизмы удаления данных.

Бронзовый солдат

В 2007 году Эстония переместила памятник, связанный с Советским Союзом, Бронзового солдата, из центра Таллинна на военное кладбище недалеко от города. В последующие месяцы Эстония подверглась ряду значительных кибератак. Сайты правительства Эстонии, СМИ и банки были перегружены трафиком в результате массовых атак типа «отказ в обслуживании» (DoS) и, как следствие, были отключены.

Необычный медведь

CrowdStrike утверждает, что российская организованная киберпреступная группа Fancy Bear нацелена на украинские ракетные силы и артиллерию в период с 2014 по 2016 год. Вредоносное ПО распространялось через зараженное Android-приложение, используемое артиллерийским подразделением D-30 Howitzer для управления данными о наведении.

Украинские офицеры широко использовали приложение, содержащее шпионское ПО X-Agent. Это считается очень успешной атакой, в результате которой было уничтожено более 80% украинских гаубиц Д-30.

Враги Катара

Эллиот Бройди, американский республиканский сборщик средств, в 2018 году подал в суд на правительство Катара, обвинив его в краже и утечке его электронной почты в попытке дискредитировать его. Катарцы якобы видели в нем препятствие на пути к улучшению своего положения в Вашингтоне.

Согласно иску, брат катарского эмира якобы организовал кампанию кибервойны вместе с другими лидерами Катара. 1200 человек стали жертвами одних и тех же нападавших, многие из которых были известными «врагами Катара», включая высокопоставленных чиновников из Египта, Саудовской Аравии, Объединенных Арабских Эмиратов и Бахрейна.

Как бороться с кибервойной

Правовой статус этой новой области все еще неясен, поскольку нет международного права, регулирующего использование кибер-оружия. Однако это не означает, что кибервойны не рассматриваются законом.

Центр передового опыта в области совместной киберзащиты (CCDCoE) опубликовал Таллиннское руководство - учебник, посвященный редким, но серьезным киберугрозам . В этом руководстве объясняется, когда кибератаки нарушают международное право и как страны могут реагировать на такие нарушения.

Проведение оценки рисков с помощью Cyber Wargames

Лучший способ оценить готовность страны к кибервойне - это провести реальное упражнение или симуляцию, также известную как кибервойна.

Военная игра может проверить, как правительства и частные организации реагируют на сценарий кибервойны, выявить бреши в защите и улучшить сотрудничество между организациями. Что наиболее важно, варгейм может помочь защитникам научиться действовать быстро, чтобы защитить критически важную инфраструктуру и спасти жизни.

Кибервойны могут помочь городам, штатам или странам повысить готовность к кибервойне за счет:

- **Тестирование различных ситуаций** - например, обнаружение атак на ранних стадиях или снижение рисков после того, как критическая инфраструктура уже была взломана.
- **Тестирование необычных сценариев** - атаки никогда не проводятся «по книжке». Создав красную команду, которая действует как

атакующие и пытается найти творческие способы взломать целевую систему, защитники могут научиться уменьшать реальные угрозы.

- **Разделение труда и механизмы сотрудничества** - кибервойна требует сотрудничества многих людей из разных организаций и государственных структур. Кибервойм может объединить людей, которые могут не знать друг друга, и помочь им решить, как работать вместе в случае кризиса.
- **Совершенствование политики** - правительства могут устанавливать политику кибервойны, но должны проверить ее на практике. Кибервойгма может проверить эффективность политик и предоставить возможность для их улучшения.

Важность многоуровневой защиты

Под давлением кибервойны правительства многих стран издали оперативную политику национальной безопасности для защиты своей информационной инфраструктуры. Эти политики обычно используют многоуровневый подход защиты, который включает:

- Обеспечение безопасности киберэкосистемы
- Повышение осведомленности о кибербезопасности
- Продвижение открытых стандартов противодействия киберугрозам
- Внедрение национальной системы обеспечения кибербезопасности
- Работа с частными организациями для улучшения их возможностей кибербезопасности

Обеспечение безопасности частного сектора

Стратегическим фактором кибервойны является устойчивость местного бизнеса к кибератакам. Компаниям необходимо ужесточить меры безопасности, чтобы уменьшить преимущества атаки на национальное государство. Ниже приводится набор мер по обеспечению корпоративной

кибербезопасности, которые могут способствовать национальной безопасности:

- Создавать препятствия для взлома сети
- Используйте брандмауэры веб-приложений (WAF) для быстрого обнаружения, расследования и блокировки вредоносного трафика.
- Быстро реагировать на нарушения и восстанавливать бизнес-операции
- Содействовать сотрудничеству между государственным и частным секторами
- Используйте местных хакеров в качестве ресурса для защиты от иностранных киберугроз.

Список литературы

1. Война в киберпространстве: уроки и выводы для России [Электронный ресурс] // Круглый стол в редакции «Независимого военного обозревателя». - Режим доступа : http://nvo.ng.ru/concepts/2013-12-13/l_war.html.
2. Госучреждения Германии страдают от хакерских атак [Электронный ресурс]. - Режим доступа : http://www.dw.de/ госучреждения-германии-страдают-от-хакерских-атак/a-16691699.
3. Дубов Д. Підходи до формування тезаурусу у сфері кібербезпеки / Д. Дубов // Політичний менеджмент. - 2010. - № 5. - С. 19-37.
4. Кибервойна: вымысел или реальность [Электронный ресурс] // Журнал Безопасность. - Режим доступа : http://www. securityinfowatch. ru/view.php? section=news&item= 121.
5. Кибернетическая безопасность и свобода информации [Электронный ресурс]. - Режим доступа : http://mediakritika.by/ article/kiberneticheskaya-bezopasnost-i-svoboda-informacii.
6. Ковалёв Н. «Началась новая техногенная эпоха - с кибервойнами, кибертерроризмом, киберпреступностью» [Электронный ресурс] / Н.

Ковалёв // Интервью для интернет-газеты «Столетия». - Режим доступа : http://www. stoletie.ru/.

7. Матвиенко Ю. А. Предупредить - значит вооружить (кибертерроризм вчера, сегодня и завтра) / Ю. А. Матвиенко // Геополитика. - 2011. - Вып. VI. - С. 59-82.
8. Мережко А. А. Конвенция о запрещении использования кибевойны в глобальной информационной сети информа-ционных и вычислительных ресурсов (Интернете) [Электронный ресурс] / А. А. Мережеко // Політичний менеджмент. - Режим доступа : http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57.
9. Министерство обороны США разрабатывает новые оперативные концепции защиты киберпространства [Электронный ресурс]. - Режим доступа : http://itstrateg.net/news/ministerstvo-oborony-ssha-razrabatyvaet-novye-operativnye-kontseptsii- zashchity-kiberprostranst.

Bibliography

1. War in cyberspace: lessons and conclusions for Russia [Electronic resource] // Round table edited by the Independent Military Observer. - Access mode: http://nvo.ng.ru/concepts/2013-12-13/l_war.html.
2. State institutions in Germany suffer from hacker attacks [Electronic resource]. - Mode of access : http://www.dw.de/ governmental-institutions-of-germany-suffer-from-hacker-attacks/a-16691699.
3. Dubov D. Approach to molding the thesaurus in the field of cybersecurity / D. Dubov // Political management. - 2010. - No. 5. - S. 19-37.
4. Cyberwar: fiction or reality [Electronic resource] // Journal of Security. - Access mode : http://www. security info watch. en/view.php? section=news&item=121.
5. Cybernetic security and freedom of information [Electronic resource]. - Access mode: http://mediakritika.by/article/kiberneticheskaya-bezopasnost-i-svoboda-informacii.

6. Kovalev N. “A new technogenic era has begun - with cyberwars, cyberterrorism, cybercrime” [Electronic resource] / N. Kovalev // Interview for the Internet newspaper “Centuries”. - Access mode : http://www. stoletie.ru/.
7. Matvienko Yu. A. To warn is to arm (cyberterrorism yesterday, today and tomorrow) / Yu. A. Matvienko // Geopolitika. - 2011. - Issue. VI. - S. 59-82.
8. Merezhko A. A. Convention on the prohibition of the use of cyber warfare in the global information network of information and computing resources (Internet) [Electronic resource] / A. A. Merezhko // Political management. - Access mode: http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57.
9. The US Department of Defense is developing new operational concepts for the protection of cyberspace [Electronic resource]. - Mode of access: http://itstrateg.net/news/ministerstvo-oborony-ssha-razrabatyvaet-novye-operativnye-kontseptsii-zashchity-kiberprostranst.

© Казарян К.К., Белан В.В., 20221 Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.

Для цитирования: Казарян К.К., Белан В.В. КИБЕРВОЙНА// Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.