КИБЕРВОЙНЫ

Мадаминова Махлиё
mahliyoxon888@gmail.com
Ташкентский государственный юридический универститет,
факультет уголовного правосудия, 1 курс, студентка Б-потока, 2 группа
https://doi.org/10.5281/zenodo.16153657

Аннотация.

Это статья посвящена анализу концепции кибервойны как современного угрозы для глобальной безопасности. В ней рассматриваются основные аспекты кибервойны, включая её определение, особенности, виды и последствия для стран и международных отношений. Особое внимание уделяется кибератакам на критическую инфраструктуру, шпионажу, саботажу, манипуляциям с информацией и пропаганде. В статье анализируются примеры реальных кибератак, а также угрозы, которые они представляют для военной, экономической и политической стабильности государств. В обсуждении рассматриваются ключевые вызовы и пути защиты от киберугроз, включая необходимость международного сотрудничества, развитие правовых норм и совершенствование технологий защиты. Статья подчеркивает важность комплексного подхода в борьбе с кибервойной и обеспечения безопасности в цифровую эпоху. А также проведем сравнительный анализ статистики кибервойн между государствами и рассмотрим несколько примеров в международном сфере и в Узбекистане по данной теме.

Ключевые слова.

«Кибервойна», «киберпространство», «кибератаки», «информационная защита», «инфраструктура», «хакерские атаки», «манипуляция информацией», «шпионаж», «саботаж», «DDoS атаки»

Введение

Важно отметить тот факт, что в XXI веке, когда технологии стали неотъемлемой частью нашей жизни, война перешла из традиционных обычных полей сражения в цифровое пространство. Это способствовало увеличению роста анонимных конфликт между государств и вызвало рост атак на внутреннюю систему государства. Перед тем как раскрыть опасность кибервойны нам следует разъяснить понятие кибервойны, и в этом мы можем рассмотреть что, кибервойна -это не просто включает в себя хакерские атаки, а является новым видом военных действий, направленный на достижение политических, экономических, и военных целей в киберпространстве. Отличительная сторона кибервойн от классических войн, это противостояние происходит не на открытой территории, а она ведется в бесформенном и неуловимом киберпространстве. Это делает ее опасной и сложной для контроля, которой представляет собой серьёзную угрозу для государств и обществ.

Современные войны отражают тенденции развития социального ума, переходят из реального пространства с вооруженными конфликтами в информационное киберпространство и является инструментом воздействия не только на физическое, но и на психологическое здоровье населения. (Битьюй, 2024).

Актуальность статьи заключается в том, что постоянный рост кибератак превращаются в реальную угрозу для государств, бизнеса и отдельных граждан, сделав

тему кибервойны крайне актуальной для усовершенствования систем защиты и подготовки специалистов. В свою очередь, современное общество во все большой степени зависит от цифровых технологий, это делает его уязвимым для кибервойны и понимания рисков и способов их предотвращения. Вот почему важно провести углубленное исследование того, как понять особенности и влияние кибервойны на современный мир и изучить методы борьбы с кибервойны.

Цель исследования- рассматривать определение, признаки, возможные последствия кибервойны и меры противодействия этой глобальной угрозе в современном цифровом мире. Для достижения поставленной цели были поставлены следующие задачи:

- Определение понятие и содержание термина «кибервойна»;
- Познакомиться с типами кибервойны и изучение угроз и рисков кибератак;
- Оценка реальных примеров кибервойны;
- Основные цели кибервойны;
- Рекомендации по успешному внедрению кибербезопаности;

Это в свою очередь, открывает путь к пониманию природы последствий кибервойны, который поможет предпринять шаги для усиления кибербезопастности и защиты от потенциальных атак.

Методы

Это исследование было проведено с использованием количественных и качественных методов для всестороннего изучения опасности кибервойны и меры противодействия к нему. Использовались следующие методы исследования:

Анализ литературы: На основе научных статьей, книг и других источников в области кибервойны изучены теоретические основы темы. Использовались такие баз данных, как Google Yandex, Google Scholar, Science web. В процессе анализа осуществлялся поиск по таким ключевым словам, как «кибервойна», «киберпространство», «информационная угроза», «информационная война», а источники, опубликованные за последние 10 лет, отбирались в приоритетном порядке.

Опрос: Был проведен онлайн-поиск для определении где именно происходит больше всего кибервойны. В этом были изучены около 60 сайтов и был внесен вывод что, из 50 стран по общему баллу всемирного индекса кибервойн, Россия заняла первое место, за ней следуют Украина, Китай, США, Нигерия и Румыния (bruce et al., 2024). Каждая из этих стран занимает свое место в первую десятку по каждой категории угроз.

Кейсы: Были изучены 2 реальных кейсов отнесённые к кибервойне. Эти кейсы были глубоко проанализированы, рассмотрены сайты и расширенно объяснено суть темы. Всего было рассмотрено около 120 сайты которое подробно рассказывает о кибервойне.

Результаты:

В результате исследования изучены ключевая информация о кибервойне. Кибервойна и есть новое явление, представляющий собой использование компьютерных сетей для осуществления атак на государственные и гражданские инфраструктуры, который может быть причиной серьезных последствий, включающих

разрушению критических систем и даже человеческие жертвы. Государства стараются создать новые стратегии защиты и ответных действий, в случаи глобализации и увеличения числа кибератак, что требует международного сотрудничества для противодействия угрозам эффективно.

Выделяются следующие 7 типы атак кибервойны:

1) **Шпионаж**- это мониторинг других стран целю которого является кража секретов, в кибервойне это включает себя использования ботнетов (по-другому «армия зомби», это устройство представляющий собой компьютерные ресурсы, которые можно использовать для разных вредоносных целей, чаще всего для рассылки спама и DDoS-атак) для компромисса конфиденциальных компьютерных систем до того, как будет украдена конфиденциальная информация.

2) **Саботаж**- информация, правительственных организаций, могут быть украден враждебном правительством или террористами, которые даже могут её уничтожить или использовать инсайдерские угрозы, такие как недовольные или неосторожные сотрудники или государственные служащие, связанные с атакующей страной.

3) **DDoS** (Distributed Denial of Servis) **«отказ в обслуживании»**- наводняет веб-сайт поддельными запросами и заставит его обрабатывать эти запросы, которые предотвращают доступ законных пользователей к веб-сайту, делав этот инструмент популярным оружием для кибер-вандалов, вымогателей и всех, кто хочет предъявить претензии. В отличие от других типов кибератак, они не пытается проникнуть за границы безопасности.

4) **Электросеть**- позволяет злоумышленникам нарушить работы инфраструктуры и потенциально нанести телесные повреждения, отключив критические важные системы. Атаки на электросеть нарушают связь и сделают такие услуги, как текстовые сообщения и связь, непригодными для использования.

5) **Пропагандистские атаки**-они включают себя распространения дезинформации, создание ложных нарративов и подрыв доверия к государственным институтам. Они обычно используются для негативного восприятия врага, и осуществляется через социальные сети и СМИ

6) **Экономический кризис**- на сегодняшний день экономическая система государств тесно связаны с компьютерами, давая к злоумышленникам возможность атаковать компьютерные сети экономических учреждений, таких как фондовые рынки, платежные системы и банки, для того чтобы украсть деньги или заблокировать доступ к необходимым средствам людей.

7) **Дезинформация**-для подрыва доверия к государственным институтам и созданий общественных волнений, распространяются ложная информация. Это особа различается от других использованием поддельных профилей для распространения ложной информацию в социальных сетях и формированием вредоносных концепции на людей ("Studnet", 2022).

На основе проведенного анализа, многочисленные страны, такие как США, Великобритания, Россия, Китай, Израиль, Иран и Северная Корея обладают активными киберспособностями, что позволяет им проводить как наступательные, так и оборонительные операции. Государства увеличивают вероятность физической

конфронтации и насилия, вызванного кибероперацией или ее частью, по мере того, как они изучают ее использование и объединяют возможности (Грин, 2016). По моему мнению, неопределенность сохраняется из-за невозможности соответствия масштабам и длительности войны.

Результаты исследования показали что, наиболее активной страной в кибервойне в 2023 году является США с 262 политически мотивированных кибератаков, и следуя за ним Россия с 63 кибератаков, которые часто направленные против Украины, Германия с 59 атак, особенно нацеленные на политические и критические инфраструктуры, Великобритания 42 кибератаки, включительно хакерские атаки против государственных учреждений и Украина с 37 атаков связанный конфликтом с Россией, в том числе Китай и Иран тоже являются активными участниками кибератак, занимав свои значимые доли от общего числа инцидентов.

«На этой войне технологии очень дороги, а вот жестокость ничего не стоит. И поэтому война напоминает нам о центральной роли людей и человеческом аспекте войны» Гэвин Уайлд, старший научный сотрудник «Фонд Карнеги за международный мир». Думаю что, Уайлд акцентирует внимание на том, что несмотря на развитие технологий, в центре войны всегда остаются люди, их решения, моральные выборы и способность к насилию. Это напоминает, что война — не просто борьба машин и технологий, а прежде всего результат человеческого поведения, которое может быть жестоким и разрушительным, независимо от технологических достижений.

Говоря о выгодах, высоко технологичный шпионаж широко распространён и осуществляется ради государственной выгоды, а также коммерческой и криминальной выгоды. Исходя из результатов глубинного исследования, средняя стоимость атаки варьируется в зависимости страны, но она высока более 15 миллионов долларов в США и 6 миллионов долларов в Великобритании.

Существует ряд причин, по которым страны проводят наступательные киберопирации. Эксперт по кибербезопасности и советник НАТО, Сандро Гайкен выступает за то, чтобы государства серьёзно обратились кибервойне, поскольку многие страны рассматривают ее как привлекательную деятельность во времена войны и мира. Для укрепления своих собственных позиций многие наступательные кибероперации предполагают широкий спектр дешевых и безрисковых вариантов ослабления других стран. Использовав доступ к важным инфраструктурам тех стран, в которых технология не так развита, можно нанести вред целой экономике, изменить политические взгляды, вызвать недоразумение внутри государств или между ними, снизить их военную стабильность.

Основные цели этих атак представляет собой:

1. **Экономические**: нанесения ущерба на экономику противного государства, кража интеллектуальной собственности, которые незаконно присваивают доступ к коммерческим секретам и технологиям;

2. **Политические:** подрыв доверия к правительству, манипуляция общественным мнением, незаконное вмешательство в выборы, т.е. повлиять на политические процессы других стран и получение доступа к внутренним документам других стран;

3. **Военные:** атаки на системы связи, навигации и управления, шпионаж за военными операциями и создание хаоса в момент конфликта;

4. **Социальные:** влияние на психическое состояние населения, провокация протестов и беспорядков, создание напряженности внутри страны через распространения дезинформации и другие которые цели могут взаимосвязываться для достижения одной цели и быть причиной реальной угрозы.

По результатам анализа, 2022 году количество кибератак в семь раз увеличилось в России, причем основными объектами станут государственные учреждения, СМИ и финансовые организации. В 2023 году количество политически мотивированных атак в России увеличится на140% по сравнению с прошлым годом, а утечки данных увеличатся более чем в 11 раз. Ключевые векторы атак включают DDoS, фишинг и уязвимости приложений. Стоимость кибератак растет и, как ожидалось, к 2023 году составил 21% по сравнению с предыдущим годом (TADVISER.ru, 2024). Хотя в Узбекистане не так была развита кибервойна, но его малейшие виды такие как онлайн мошенничество и кража банковских карт составляет 70% всех инцидентов. В 2023 году было закреплено около 5500 киберпреступлений, что указывает на необходимость повышения цифровой грамотности населения и усиления мер безопасности. (podrobno.uz, 2024).

Обсуждение:

Результаты исследования подтвердили, что за последние десятилетия произошло множество крупных кибератак, которые не только нарушали внутреннюю информационную систему и деятельность государств, но и проверили устойчивость и сила международного права.

«Контроль над кибервооружением невозможен, а чем выше уровень технологического развития общества, тем более уязвимым оно становится. Кроме того, опасность искусственного интеллекта на службе политиков в том, что у него нет ни психологии, ни морали, а есть только цели и задачи» - бывший госсекретарь США Генри Киссинджер.

Stuxnet и Иран: 2010 год ознаменовал начало совершенно нового типа военных действий-кибернетических. В сентябре этого же года стало известно, что компьютерный вирус Stuxnet нанес значительный ущерб иранской ядерной программе. Этот червь весом в 500 килобайт стал причиной повреждения 1368 из 5000 центрифуг для обогащения урана и отбросил ядерную программу Ирана примерно на два года назад. Ещё раз: 500 килобайт кода на ассемблере, C и C ++ частично разрушили инфраструктуру ядерной программы целой страны, которую выстраивали на протяжении десятилетия. По уровню ущерба действие червя можно сравнить с полноценным налётом ВВС и атакой воздуха (habr.com, 2021). При этом нет никакого риска для живой силы атакующего и военной техники, не тратятся боеприпасы. Для атаки не нужно ничего, кроме куска кода. Несмотря на то что, уже прошло 10 лет после первого звоночка кибервойн, но до сих пор неясно, насколько серьёзный ущерб могут причинить подобные атаки. Эксперты рассматривают самые пессимистичные варианты вроде подрыва ядерных боеголовок прямо в шахтах запуска.

Россия и Украина: Результаты анализа показали что, в течение 2022 года число кибератак против украинских пользователей выросло в 2.5 раза, а пользователей в странах НАТО – в 3 раза. Но известно своим названием «скрытая» война началось в январе 2022 года, Украина встретилась с массированной хакерской атаке, нацеленной на правительскую инфраструктуру, которые повторились и в феврале. Украина обвиняет Россию причастности к проникновению около 70 государственных сайтов, включая украинского МИДа, а также министерство образования и науки. Была создана масштабная многомесячная российская компания для уничтожения энергетической системы Украины. Россия представляла кибервойну в качестве интегральной частью своей военной структуры, а не дополнением или отдельным инструментом. Но правительство Украины начались готовить для отражения кибератак. Как сказал Михаил Федоров, бывший Министр цифровой трансформации Украины, что в 2021 году для того чтобы атаковать украинский государственный сайт Киев платил огромное количество денег хакерским группам, после того как архитектура сайта было идеально выстроена для военного времени. В начале 2023 года должностные лица Украины провозгласили, что они будут обратиться в международный суд в Гааге с доказательствами, чтобы их признали военными преступлениями. В конце концов, суд выявлял что эти являются военными преступлениями, поскольку они направлены против мирного населения. Власть России, со своей стороны, не исключают возможности освободить хакеров от ответственности. 10 февраля глава комитета Государственной думы по информационной политике, Александр Хинштейн призвал освободить от уголовной ответственности тех хакеров, которые «действуют в интересах Российской Федерации». Но сам Уголовный Кодекс Российской Федерации предусматривает для киберпреступников наказание до 7 лет тюрьмы.

«Кибероперации не изменили войну. Но изменили наше представление об определённых аспектах ведения войны. Несмотря на разговоры об этом в течение 30 лет, это первый раз, когда можно видеть в реальном времени, какой вклад кибербезопасность вносит в масштабную военную кампанию» Тим Стивенс, доцент, Королевский колледж Лондона. Я предполагаю что, он имел ввиду, что важным аспектом современных войн, мы можем наблюдать их реальное влияние на ходы масштабных конфликтов. Причиной этого может служить стремительное развитие технологии, особенно в сфере кибербесопасности, которые позволяет государствам эффективно работать над киберпространствой как часть военных стратегий. И по его словам кибероперации не заменяют традиционные формы введения войны, они могут значительно изменять методы воздействия.

Рекомендации по успешному внедрению кибербезопаности:

Чтобы обеспечить кибербезопасность государствам нужны предпринять некоторые комплексные шаги на различных уровнях. На основе проведенной исследовании, мы рассмотрим основные меры, которые нужно принять:

1. **Образование и осведомлённость** – программы обучения и тренировки для сотрудников и граждан по вопросам киберугроз и разработка культуры безопасности, чтобы все сотрудники и пользователи понимали важность соблюдения кибербезопасности на высоком уровне.

2. **Технические средства обеспечивающие кибербезопасности** – постоянное обновление антивирусные и антишпионские программы для защиты от вирусов, шпионских программ и других атак и защита сетевой инфраструктуры от несанкционированного доступа, а также подтверждению многофакторной аутентификации.

3. **Тестирование и аудиты** – регулярно проведений тестов на уязвимости с помощью регулярных аудитов и постоянная оценка рисков поможет выявить уязвимости и адаптировать защиту.

Устав ООН

Основная правовая рамка, который регулирует кибервойну это Устав ООН. Устав ООН является фундаментом международного права, относящихся к кибервойне и основывается на принципах государственный суверенитет и запрет применения силы или угрозы силой. Статья 2(4) Устава запрещает государствам применять силу против территориальной целостности или политической независимости любого государства или любым другим способом, несовместимым с целями Организации Объединенных Наций. Применительно кибероперациям любое действие, которое существенно нарушает важнейшие функции другой страны, может рассматриваться как нарушение этого принципа.

Международное гуманитарное право

Следующим видом право, которое имеет международный характер является Международное гуманитарное право (МГП), также известное как право вооруженных конфликтов, применяется к ведению войны и защите людей во время войн. Принципы различия, пропорциональности и необходимости определяют, проводятся ли и каким образом кибероперации во время вооруженных конфликтов. Кибероперации во время войны, нацеленные на гражданскую инфраструктуру и не дающие явного военного преимущества, могут нарушать МГП.

Таллиннское руководство

Хотя Таллиннское руководство и не имеет обязательной юридической силы, оно представляет собой значимую научную работу по международному праву, применимому к кибервойне. Руководство, разработанное учеными-юристами и практиками, подробно изучает, как международное право применяется к киберконфликтам и кибервойнам, предлагая интерпретации и рекомендации по таким вопросам, как суверенитет, ответственность государств, а также морское и воздушное право в контексте киберпространства. (medium.com, 2024)

В глобальном индексе кибербезопасности, который было составлено экспертами Международного союза электросвязи ООН (International Telecommunication Union) из стран Центральной Азии наиболее высокую позицию в 2020 году занимал Казахстан-38 место из 192 стран. Далее идет Узбекистан – 78, Кыргызстан — 100, Таджикистан в этом рейтинге на 146 месте. Подводя итоги вышесказанных, можно отметить, что Узбекистан тоже уделяет большое внимание развитию цифрового сектора, приводя пример можно сказать, что в 2022 году был принят Закон Республики Узбекистан «О Кибербезопасности», который дал толчок развитию образования в области

цифровизации среди населения, обратить пристальное внимание на подготовку кадров и усилить работу по защите собственного цифрового пространства.

Заключение

По итогу проведенной попытки анализа было раскрыто понятие и содержание кибервойны, было ознакомлено с типами кибервойны и их угрозой, даны оценки реальных угроз кибервойны, были перечислены и рассмотрены основные цели кибервойны, также соответствующим были даны рекомендации по развитию и внедрению кибербезопасности.

Данное исследование продемонстрировало, что кибербезопасность — это не единичная задача, а долгосрочный процесс, требующий постоянного обновления знаний, технологий и методов защиты. Мы также провели сравнительный анализ между государствами и рассмотрим несколько примеров в международном сфере и в Узбекистане по данной теме, кроме того, рассмотрены результаты работы, которые были проведены в Узбекистане последние годы по обеспечению кибербезопасности.

Подводя итоги на исследования, могу сказать что, кибервойна требует комплексного подхода, включающего не только технологические решения, но и правовые, политические и этические аспекты, чтобы минимизировать риски и последствия для международной безопасности.

References:
Используемая литература:
Foydalanilgan adabiyotlar:

1. Кэтлин холл Джеймисон (2018), Кибервойна: Как российские хакеры и тролли помогли избрать президента.
2. Виктор Нечипуренко, Валерий Касьянов(2023). Социология Интернета 2-ое издание, Учебник для ВУЗов.
3. https://roscongress.org/materials/ , Кибервойна уже идёт?
4. https://www.tadviser.ru/,(2024)Обнаружена волна кибератак
5. hteps://podrobno.uz/,(2024), Кибер-романтика и письма из Нигерии. Как и почему узбекистанцы становятся легкой мишенью для мошенников в интернете.
6. https://medium.com/, (2024) What is cyber Warfare?
7. https://timesofindia.indiatimes.com, (2022) The real story behind Russia-Ukraine cyber wars.
8. https://www.sciencefocus.com/
9. https://cabar.asia/ru/. Экспертная встреча: Кибербезопасность в странах Центральной Азии. Что делается для ее улучшения?
10. https://habr.com/ru/ (2021) Кибервойна. Когда 500 Кб кода страшнее межконтинентальной ракеты.
11. https://www.securitylab.ru/. (2023) Кибервойна: Понимание современной угрозы в цифрофую эру.
12. https://dzen.ru/. (2022)Что значит кибервойна?
13. https://www.currenttime.t/. (2016) Кибервойны: зачем страны набирают армии хакеров?