O‘ZBEKISTON RESPUBLIKASI
MUDOFAA VAZIRLIGI

AXBOROT – KOMMUNIKATSIYA TEXNOLOGIYALARI VA ALOQA HARBIY INSTITUTI

“IT-XAVFSIZLIK QALQONI. HARBIY SOHAGA AXBOROT TEXNOLOGIYALARINI INTEGRATSIYA QILISHDAGI MUAMMO VA YECHIMLAR”

MAVZUSIDAGI RESPUBLIKA ILMIY-AMALIY KONFERENSIYASI
MAQOLALAR TO‘PLAMI

СБОРНИК СТАТЕЙ
РЕСПУБЛИКАНСКОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ

«IT-ЩИТ БЕЗОПАСНОСТИ. ПРОБЛЕМЫ ПРИ ИНТЕГРАЦИИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ВОЕННУЮ СФЕРУ И ИХ РЕШЕНИЯ»

2024 yil 27 - MART

Konferensiya tashkiliy qo‘mitasining
T A R K I B I:

general-mayor Qarshiyev H.A.	O‘R Mudofaa vazirining tarbiyaviy va mafkuraviy ishlar bo‘yicha o‘rinbosari
polkovnik Mamadaliyev U.O.	O‘R Mudofaa vazirligi harbiy kadrlarni tayyorlash boshqarmasi boshlig‘i
podpolkovnik O‘rmonov B.B.	O‘R QK BSH Aloqa, axborot texnologiyalari va axborotlarni himoyalash bosh boshqarmasi boshlig‘i
podpolkovnik Raximov B.N.	Rais, O‘R MV AKT va AHI boshlig‘i, t.f.d., professor
polkovnik Mirjalolov O.A.	Rais o‘rinbosari, O‘R MV AKT va AHI boshlig‘ining o‘quv va ilmiy ishlar bo‘yicha birinchi o‘rinbosari, PhD, dotsent
kapitan To‘rayev B.Z.	O‘R MV AKT va AHI boshlig‘ining o‘rinbosari-Kiberxavfsizlik fakulteti boshlig‘i, t.f.d., professor
polkovnik Davlatov O‘.R.	O‘R MV AKT va AHI boshlig‘ining o‘rinbosari-shtab boshlig‘i
podpolkovnik Shermatov F.T.	O‘R MV AKT va AHI boshlig‘ining tarbiyaviy va mafkuraviy ishlar bo‘yicha o‘rinbosari, PhD, dotsent
polkovnik Nurmatov T.Sh.	O‘R MV AKT va AHI malaka oshirish fakulteti boshlig‘i, dotsent
QK xizmatchisi Muxitdinov X.A.	O‘R MV AKT va AHI ilmiy - tadqiqotlar laboratoriyasi yetakchi ilmiy xodimi, i.f.n., professor
QK xizmatchisi Nazarov A.M.	O‘R MV AKT va AHI ilmiy - tadqiqot laboratoriyasi yetakchi ilmiy xodimi, t.f.d., professor
QK xizmatchisi Sultanov D.I.	O‘R MV AKT va AHI ilmiy – tadqiqot laboratoriyasi yetakchi ilmiy xodimi, h.f.d., katta ilmiy xodim
QK xizmatchisi Qurbonov Sh.K.	O‘R MV AKT va AHI ilmiy - tadqiqot laboratoriyasi katta ilmiy xodimi, t.f.n., dotsent
mayor Tajiyev J.A.	O‘R MV AKT va AHI ilmiy - tadqiqot laboratoriyasi boshlig‘i, PhD, dotsent
podpolkovnik Tashtayev Z.D	O‘R MV AKT va AHI metodik bo‘lim boshlig‘i
mayor Kuzibekov N.Ch.	O‘R MV AKT va AHI o‘quv bo‘limi boshlig‘i

polkovnik Bazarov A.B.	O‘R MV AKT va AHI kafedra boshlig‘i, PhD, dotsent
polkovnik Mamaraufov O.A.	O‘R MV AKT va AHI kafedra boshlig‘i, dotsent
podpolkovnik Nishanov I.P.	O‘R MV AKT va AHI kafedra boshlig‘i, PhD
podpolkovnik Tursunov Q.M.	O‘R MV AKT va AHI kafedra boshlig‘i, PhD, dotsent
podpolkovnik Mirvaliyev I.B.	O‘R MV AKT va AHI kafedra boshlig‘i, dotsent
podpolkovnik Nurmetov B.S.	O‘R MV AKT va AHI kafedra boshlig‘i, PhD
kapitan Turapov Sh.N.	O‘R MV AKT va AHI kafedra boshlig‘i, PhD, dotsent
kapitan Yusupov B.K.	O‘R MV AKT va AHI kafedra boshlig‘i, PhD, dotsent
podpolkovnik Abdiroziqov O.Sh.	Kotib, O‘R MV AKT va AHI kafedra katta o‘qituvchisi, PhD, dotsent
mayor Jumagaldiyev S.I.	O‘R MV AKT va AHI ilmiy - tadqiqot laboratoriyasi ilmiy xodimi
kapitan Komilov A.A.	O‘R MV AKT va AHI kafedra katta o‘qituvchisi
katta leytenant Boboyev N.T.	O‘R MV AKT va AHI kafedra katta o‘qituvchisi, PhD
QK xizmatchisi Abidov A.A.	Kotib, O‘R MV AKT va AHI kafedra dotsenti, dotsent
QK xizmatchisi Sapayev Sh.R.	O‘R MV AKT va AHI kafedra dotsenti
QK xizmatchisi Umaraliyev B.N.	O‘R MV AKT va AHI kafedra katta o‘qituvchisi
III darajali serjant Axmedov Z.M.	O‘R MV AKT va AHI kafedra katta texnigi

66.	**NAZIMOV R. N. XOLMATOV N. M.** Ta’lim-tarbiya jarayonida interfaol metodlardan foydalanishga doir ilg‘or xorij tajribasi …….	**325**
67.	**KARIMOV Sh.I.** Markaziy Osiyo davlatlarining tarkib topishi, hududi va chegaralari…… ……..……..	**330**
68.	**KARIMOV Sh.I.** Markaziy Osiyoning geografik xususiyatlari…...……...	**333**
69.	**АТАЖАНОВА О.И., КУРБАНБАЕВ Ш.Э.** Алоқа воситалари жойлашган бино ва иншоатларда юқори дисперс волластонит минераллари асосида бетон материаллар олиш ва уларнинг физик-механик хоссаларини тадқиқ этиш……...	**338**
70.	**АТАЖАНОВА О.И., КУРБАНБАЕВ Ш.Э.** Ультратовушли дефектоскопда бетон асосли материалларнинг алока воситалар сакланувчи биноларда термик бардошлилигини аниклаш бўйича тадқиқотлар…….	**342**
71.	**ВАЛИУЛИН А.Ш.** Использование военными организациями сетей darknet и deepweb в стратегии кибервойн…….	**346**
72.	**DJABBAROV SH. YU., XAMDAMOV D.B**. Korporativ tarmoq xavfsizligi arxitekturasi va bo‘lishi mumkin bo‘lgan hujumlar yo‘nalishlari…….	**354**
73.	**DJABBAROV SH. YU., XAMDAMOV D.B**. Ma’lumot uzatish tarmoqlarida axborot xavfsizligini ta’minlash xususiyatlari va muammolari ……	**358**

5. Сулейманов А.А. ИЗМЕРЕНИЕ АСПИРАЦИОННЫХ ПОТОКОВ, ОБРАЗУЮЩИХСЯ ПРИ ПОЖАРАХ Справочник. Инженерный журнал. 2019. № 2 (263). С. 42-48.

6. Петросова Л.И, Одилова М.О. Пути улучшения подготовки специалистов по "Безопасность жизнедеятельности". Научно-практический Журнал «Фан. Мухофазаса, хавфсизлик». 2 (1-2), -С 120-125.

ИСПОЛЬЗОВАНИЕ ВОЕННЫМИ ОРГАНИЗАЦИЯМИ СЕТЕЙ DARKNET И DEEPWEB В СТРАТЕГИИ КИБЕРВОЙН

Специалист ГУП «Центр Кибербезопасности»
Валиулин А.Ш.

Аннотация. *В статье рассматриваются особенности использования военными организациями сетей Darknet и DeepWeb для сбора разведывательной информации, саботажа, кампаний по дезинформации, безопасной связи, вербовки негласных помощников.*

Ключевые слова: *Кибервойна, Darknet, DeepWeb, Surface Web, луковая маршрутизация, Tor.*

Annotatsiya. *Maqolada harbiy tashkilotlar tomonidan Darknet va DeepWeb tarmoqlaridan razvedka ma'lumotlarini to'plash, sabotaj, dezinformatsion kampaniyalar, xavfsiz aloqalar va maxfiy yordamchilarni yollash uchun foydalanish xususiyatlari muhokama qilinadi.*

Kalit so'zlar. *kiber urush, Darknet, DeepWeb, Surface Web, piyoz marshrutlash, Tor.*

В последние годы Darknet превратился в тайную область, где военные подразделения по всему миру проводят тайные кибероперации, используя анонимность и шифрование позволяющие пользователям и операторам сайтов оставаться недоступными для отслеживания. В настоящее время военные организации используют Darknet и DeepWeb для сбора разведывательной информации, саботажа, кампаний по дезинформации и психологических операций, безопасной связи, вербовки негласных помощников, иллюстрируя разнообразный спектр деятельности, проводимой в этих сегментах виртуального пространства.

Опираясь на примеры из различных регионов и конфликтов, можно рассмотреть механизмы, используемые военными подразделениями в сети Darknet, а также провести анализ последствия эксплуатации Darknet ресурсов для современных войн. Исследуя влияние военной эксплуатации сетей Darknet и

DeepWeb на безопасность и оборону стран, мы подчеркиваем острую необходимость всесторонних исследований и анализа этой области.

В целях дальнейшего изучения указанных сегментов виртуально пространства, приводится их определения. Так в настоящее время в связи с появлением новых технологических коммуникационных решений взаимодействия в сети интернет, виртуальное пространство разделилось на сегменты, среди которых наиболее выраженные признаки имеют три пространства: видимая сеть Surface Web, глубинная сеть Deep Web и теневая сеть Darknet или как её иначе называют теневой интернет Dark Web.

Рисунок 1. Образное представление всемирного виртуального пространства

С учетом неравномерного распределения объема информаций в отмеченных трех сетях, для наглядности представления объема и сущности разделения виртуального пространства, исследователи предложили использовать образное представление айсберга, у которого лишь 10 % находится над водой, что примерно сопоставимо с объемом информации в видимой сети Surface Web. Остальная часть айсберга, скрытая под водой, символизирует сети Deep Web и Darknet, также скрытые от обычных пользователей.

Сеть Surface Web является общедоступной интернет сетью и ее ресурсы размещаются в открытом доступе, поиск которых возможен посредством браузеров Internet Explorer, Google Chrome, Firefox, Opera и других предназначенных для просмотра содержаний сайтов открытого Интернета.

При этом сеть Deep Web представляет из себя неиндексируемые ресурсы, не предоставляющие доступ через поисковые системы. К ним относят государственные базы данных, корпоративные сайты, электронные библиотеки и др. К сайтам глубинного Интернета разрешен доступ только ограниченным пользователям по паролю или после регистрации.

Сеть Darknet это намеренно скрытое оверлейное (построенное поверх) соединение, доступное исключительно через систему прокси-серверов и не отображающееся в поисковых системах и стандартных браузерах. Данная сеть требует наличия специального программного обеспечения Tor, I2P, Freenet, Bitmessage, Perfect Dark, ANts P2P, Filetopia, Gnutella2, MUTE и д.р., создающие анонимные коммуникации посредством которых осуществляется доступ к

ресурсам теневой сети. По последним данным, объем Darknet не превышает 3-4% объема открытого Интернета. Соединения с указанной сетью устанавливаются только между доверенными узлами, с использованием шифрования.

Анализ получаемых сведений свидетельствует, о том что военные подразделения большинства стран все чаще обращаются к сетям Darknet и DeepWeb как к тайной сфере для проведения кибероперациий. Эта сфера предлагает анонимность, шифрование и обширную сеть незаконных рынков, форумов и каналов связи, что делает ее привлекательной для сбора разведывательной информации, саботажа и кампаний по дезинформации. Анализ того, как военные организации ориентируются и используют эти сегменты, имеет решающее значение для понимания современных стратегий ведения кибервойны.

Изучение количественного состава пользователей сети Tor с ее луковой маршрутизацией, являющейся наиболее распространенной в мире, свидетельствует об использовании военными подразделениями данной сети.

За последние 5 лет военизированными подразделениями многих стран стали активно использовать луковую маршрутизацию сети Tor, чтобы скрыть свои истинные намерения в виртуальном пространстве.

При этом одним из направлений использования сети Darknet в кибервойне представляющей из себя «Действия одного национального государства с проникновением в компьютеры или сети другого национального государства для достижения целей нанесения ущерба или разрушения», является получения разведывательных сведений о потенциальном противнике.

Военизированные подразделения в целях получения разведывательных сведений о вооружении, составе, стратегии вооруженных сил и иных сведений зачастую хранящихся в сети Deep Web, могут использовать луковую маршрутизацию сети Darknet. В этих целях сеть Tor выступает в качестве скрытого канала подключения и получения сведений хранящихся с на государственных серверах противника.

В связи с обработкой больших объемов данных анализ и получения разведывательных сведений о вооружении противника осуществляется специальными программными продуктами которые анализирует содержимое открытых портов сервера противника используя луковую маршрутизацию для сокрытия своего истинного месторасположения. Однако анализ диаграммы пользователей сети Tor и объемов скачиваемой информации позволяет выявлять факт использования таких программных продуктов в той или иной стране. Так при функционировании разработанных программ использующих данную сеть возникают аномалии в статистических показателях использования сети Tor. В этом контексте мы используем термин «аномалия», чтобы показать неестественное увеличение количества пользователей сети Tor, не связанное с реальными пользователями.

Анализируя аномалии, возникающие в сети Tor в определенной стране при геополитических событиях, а также возможностях военизированных подразделений, можно предположить, какая организация инициировала аномалию и в связи с чем.

Одной из главных аномалий прошлого года можно считать быстрый рост числа пользователей сети Darknet в Германии с 400 000 пользователей в день 1 июня до 2 345 000 в июле 2023 года, с данного момента Германия заняла лидирующую позицию в мире с 48,64% от общего числа пользователей во всем мире.

Данное было связанно с крупнейшей в истории НАТО учения по отработке действий по развертыванию военно-воздушных сил государств-членов. В этот период 25 стран приняли участие в двухнедельных учениях «Эйр дефендер», в которых было задействовано около 10 000 военнослужащих и 250 летательных аппаратов, учения проходили с 12 по 23 июня 2023 года.

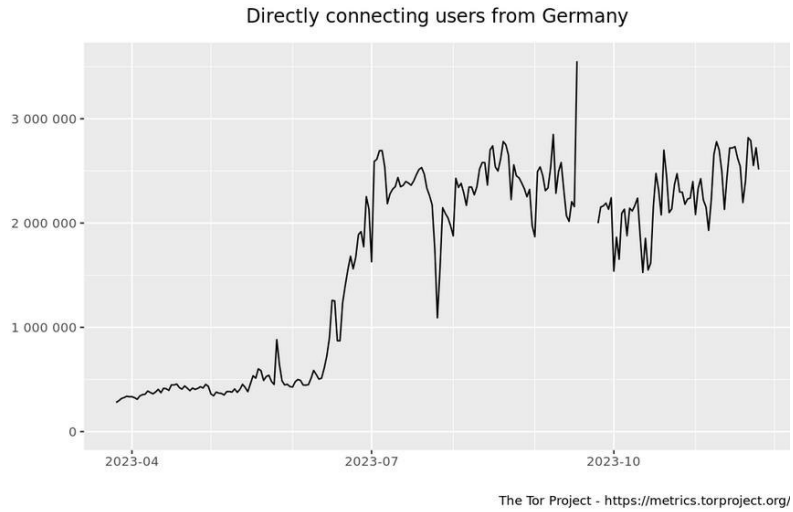

Рисунок. Количество пользователей сети Tor в Германии

График пользователей сети Tor в Германии в этот период, указывает на определённые аномалии, в частности с начала учений наблюдается рост который указывает на использование военнослужащими не только самого Tor браузера, но и на то что были запущенны определенные программные продукты используемые луковую маршрутизацию указанной сети. При этом в сентябре 2023 года данное оборудование после испытания на максимальное соединение которое составило более 3,5 млн пользователей дало определенный сбой всей сети Tor, который длился несколько дней.

С учетом того, что технологию луковой маршрутизации в 1998 году запатентована Военно-морскими силами США, а анонимная сеть Tor является доминирующей сетью использующей данную технологией, не удивительно что военные подразделения НАТО активное используют сеть Darknet.

Кроме того НАТО признали стратегическую важность сети Darknet в современной войне и включили сбор разведывательной информации и кибервозможности данной сети в свои оборонные стратегии. К примеру Центр

НАТО по сотрудничеству в сфере кибероборонь (NATO Cooperative Cyber Defence Centre of Excellence), базирующийся в Эстонии, проводит исследования и обучение методам эксплуатации сети Darknet с целью повышения способности государств-членов обнаруживать и смягчать киберугрозы, исходящие из киберпространства. Аналогичным образом Киберкомандование США создало специальные подразделения, которым поручено отслеживать и препятствовать действиям противника в сети Darknet, рассматривая данную сеть как поля битвы киберпространства.

Как было отмечено одним из основных способов использования сети Darknet военными организациями являются операции по сбору разведывательной информации. Используя функции анонимности и шифрования, военные организации по всему миру могут тайно собирать конфиденциальную информацию о противниках, начиная от их военного потенциала и заканчивая их стратегическими намерениями. Например, Силы обороны Израиля (ЦАХАЛ) используют платформы сети Darknet для мониторинга деятельности враждебных группировок, таких как «Хезболла» и «Хамас», собирая информацию об их тактике вербовки, оперативных планах и финансовых сетях. Благодаря тайному проникновению на форумы сети Darknet и каналы связи подразделение 8200 (израильское подразделение радиоэлектронной разведки, входящее в Управление военной разведки «АМАН»), отвечающее за радиоразведку и кибервойну, смогло превентивно получить разведывательные сведения о противнике.

Таким образом, возможности сбора разведывательной информации, получаемые посредством сети Darknet, играют ключевую роль в современных военных операциях, позволяя военным организациям получать ценную информацию о действиях и намерениях противника. Будь то мониторинг террористических организаций, проведение кибершпионажа против иностранных правительств или сбор боевых разведывательных данных в зонах конфликтов.

Еще одним из направлений использование сети Darknet при военных конфликтах можно считать распространения оружия среди населения при вооруженных конфликтах. Так с сети Darknet имеются множество платформ распространяющие оружие, информацию о методах ее изготовления, продаются поддельные документы, оружие, взрывчатка, в закрытых чатах террористическими и экстремистскими структурами обсуждаются меры по дестабилизации обстановки, а также проведению террористических актов, дискредитации правительств.

Так в сети Darknet активно распространяется оружие и взрывчатые вещества, в качестве примеров можно привести отдельные торговые площадки и сайты сети Darknet, занимающиеся незаконным оборотом оружия и взрывчатых веществ.

В частности, торговая площадка Deep Gun Guns Store armoryohajjhou5m.onion предлагает малокалиберное и крупнокалиберное

оружие. Данный сайт специализируется на продаже автоматического оружия, а также снайперских винтовок. Например, АК - 47 стоит порядка 0,0202 биткоина (около 1000 долларов США).

Рисунок 2. Ресурс сети Darknet Luckp 47 shop

В связи с систематическим возникновением локальных воин и вооруженных конфликтов, теневой рынок огнестрельного оружия постоянно пополняется за счет вооружения противоборствующих сторон. В качестве примера можно привнести ресурс Luckp 47 shop администраторами которого являются граждане Украины, торгующие через указанный магазин оружием из зон конфликта на востоке Украины.

Данный сайт реализует различное огнестрельное оружие, взрывчатые вещества, гранаты и противотанковое оружие. При этом в стоимость оружия включается доставка и упаковка, а в качестве рекламного поощрения при заказе любого огнестрельного оружия покупатель получает 50 пуль бесплатно.

Следует отметить, что указанные, а также аналогичные им магазины, реализующие оружие и взрывчатые вещества, работают в рамках идентичной организационной модели.

Одной из категорий клиентов отмеченных виртуальных магазинов являются наемные убийцы т.н. «киллеры» которые активно используют сеть Darknet для рекламы своих услуг.

С учетом того, что наёмный убийца совершает убийство по заказу за вознаграждение, то анонимная сеть Darknet, позволяет обеспечить хорошее алиби заказчику заказного убийства. При этом, исполнитель никак напрямую не связанный ни с жертвой, ни с заказчиком, может беспрепятственно рекламировать свою деятельность в данной сети.

В качестве примеров можно привести ряд сайтов, рекламирующих услуги наемных убийц, в том числе на территории Узбекистана. Так сайт Hitman servise представляет услуги наемных убийц якобы осуществляющих убийства по всему миру включая Узбекистан, а также Китай, Северную Корею, Россию, Кубу, Иран, Ирак, Судан, Ливию, Сирию, Саудовскую Аравию, Йемен, Уганду, Таиланд.

Рисунок 3. Ресурс сети Darknet Hitman servise

Оплата, как и в большинстве ресурсов сети Darknet осуществляется только в биткойнах, а цены зависят от статуса жертвы. В качестве контактна дается электронная почта hitman4hire@vfemail.net. Исполнителем заказа якобы является бывший военный, имеющий опыт работы наёмным убийцей более 15 лет.

Теневой Интернет также активно используется террористическими и экстремистскими группировками. Фанатично настроенные группировки, несмотря на религиозные ограничения, активно используют технические новшества в своих целях. Современный терроризм обладает развитой информационно-коммуникационной инфраструктурой и демонстрирует высокий уровень владения передовыми технологиями, включая методы работы в сервисах сети Darknet.

Кроме того, в условиях ближневосточного конфликта наблюдается распространение тактики кибервойны с использованием Darkneta, когда государственные и негосударственные субъекты используют анонимность, обеспечиваемую сетью Darknet, для сбора разведывательной информации и диверсионных операций. Например, во время продолжающейся войны в Сирии как правительственные силы, так и повстанческие группировки, общаются при помощи сети Darknet, а также используют ее для закупки оружия, координации атак и распространения пропаганды, подчеркивая многогранный характер эксплуатации Darkneta в современных военных конфликтах.

Помимо этого, военные организации используют сеть Darknet для проведения диверсий и наступательных кибероперациий против противников. Этот тайный подход позволяет военным организациям по всему миру, включая государства-члены НАТО, разрушать вражеские сети, инфраструктуру и критически важные системы с высокой степенью анонимности и возможности отрицания. Например, как сообщается, Штаб правительственной связи Великобритании (GCHQ) и Агентство национальной безопасности США (АНБ) использовали сеть Darknet для проникновения и саботажа коммуникационных сетей террористических организаций, таких как ИГИЛ, с целью подорвать их командование и возможности контроля и препятствовать их способности координировать атаки.

Более того, использование Darkneta для наступательных кибероперацій выходит за рамки традиционных военных конфликтов и включает сценарии гибридной войны и асимметричных угроз. Например, спонсируемые государством хакерские группы, связанные с такими странами, как Россия, Китай и Иран, были замешаны в проведении кибератак против западных правительств, финансовых учреждений и инфраструктуры с использованием тактики, основанной технологиях сети Darknet. Эти операции могут включать в себя развертывание вредоносного ПО, проведение распределенных атак типа «отказ в обслуживании» (DDoS) или использование уязвимостей в вражеских системах, обнаруженных с помощью разведки в Darknete, что создает серьезные проблемы для безопасности и стабильности целевых стран.

Таким образом, диверсионные и наступательные операции, проводимые через сеть Darknet, представляют собой важнейший компонент современных военных стратегий кибервойны. Используя анонимность и скрытность сети Darknet, военные организации, могут срывать операции противника, снижать возможности противника и достигать стратегических целей, не прибегая к открытым действиям. Однако распространение наступательных возможностей с использованием сети Darknet также подчеркивает необходимость надежных мер кибербезопасности, международного сотрудничества и этических соображений для смягчения рисков, создаваемых конфликтами с использованием кибербезопасности во все более взаимосвязанном мире.

Подводя итог, можно сказать, что использование сети Darknet военными подразделениями для кибероперацій включает в себя кампании по сбору разведывательной информации, саботажу и дезинформации, каждая из которых обусловлена различными критериями и факторами. Понимание тонкостей использования военными подразделениями сети Darknet имеет важное значение для решения развивающихся проблем, связанных с современными стратегиями кибервойны. Анализ военного использования сети Darknet и его многогранных последствий для современной войны подчеркивает острую необходимость всесторонних исследований в этой растущей области. Решение возникающий с этой сфере проблем требует междисциплинарного сотрудничества и постоянного диалога между исследователями, политиками, экспертами по правовым вопросам, и техническими специалистами.

Использованная литература:

[1] Aldridge J., AskewR. Delivery Dilemmas: How Drug Cryptomarket Users Identify and Seek to Reduce Their Risk of Detection by Law Enforcement // Журнал Drug Policy. - London, 2017.;

[2] Barratt M.J., Aldridge J., Maddox A. The Darknet. In: Sage Encyclopedia of the Internet // Журнал Sage. - London, 2017.

[3] Bender R., Alessi C. Munich Shooter Likely Bought Reactivated Pistol on Dark Net // Информационный ресурс Wsj.com. 2017.

[4] D.S. Dolliver, J.L. Kenney Characteristics of Drug Vendors on the Tor Network // Журнал Cryptomarket Comparison. 2016.

[5] Яковлев А.Н. Цифровая криминалистика как фактор защиты цифровой экономики // Материалы международной научно-практической конференции «Криминалистика в условиях развития информационного общества». –Москва. Академия управления МВД России. 2018. С. 325-330

[6] Умаров Б.М., Қодиров У.Д., Каримов Х.К.. Очиқ ахборот тизимларида ахборот- психологик хавфсизлик // Тошкент. «Fan va texnologiya». 2012. 223б

[7] Соловьев В.С., Осипенко А.Л. Рынок нелегальных товаров и услуг в Darknet и Telegram-каналах // Уголовная политика и культура противодействия преступности: сборник материалов Международной научно-практической конференции. - Краснодар, 2018. - С. 138-141. 54.

[8] Алескеров В.И. О некоторых аспектах преступлений экстремистской и террористической направленности, совершаемых с использованием сферы телекоммуникаций и компьютерной информации // Материалы международной научно-практической конференции «Криминалистика в условиях развития информационного общества». Москва. Академия управления МВД России. 2018. С. 14

[9] Сайт The Tor Project - https://metrics.torproject.org

KORPORATİV TARMOQ XAVFSIZLIGI ARXITEKTURASI VA BO‘LISHI MUMKIN BO‘LGAN HUJUMLAR YO‘NALISHLARI

T.f.n., dotsent Djabbarov Sh. Yu.
Muhammad al-Xorazmiy nomidagi TATU
dotsent, leytenant Xamdamov D.B.
O‘R MV Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti

Ushbu maqolada korporativ tarmoq arxitekturasi va bo‘lishi mumkin bo‘lgan hujumlar yo‘nalishlari keltirilgan. Hujumlarni aniqlash va amalga oshirish uchun maqsadlarni aniqlash, portlarni skanerlash, xabarlarni ushlash va ma’lumotlarni o‘g‘irlash usullari keltirilgan. Buzg‘unchilikni aniqlash uchun korporativ tatmoqning barcha elementlari o‘rtasida doimiy ma’lumot almashinuvi zarurligi ko‘rib o‘tilgan.

Kalit so‘zlar: *korporativ tarmoq, axborot xavfsizligi, ma’lumotlarning yaxlitligi, maxfiylik, ishonchlilik, taxdid, xaker, buzg‘unchi.*

Аннотация. *В этой статье представлен обзор архитектуры корпоративной сети и перечислены возможные маршруты атаки. Для обнаружения и выполнения атак предусмотрены методы определить цели, сканирования портов, перехвата сообщений и кражи данных. Для выявления нарушения была учтена необходимость постоянного обмена информацией между всеми элементами корпоративной сети.*