O‘ZBEKISTON RESPUBLIKASI ICHKI ISHLAR VAZIRLIGI AKADEMIYASI

KIBERXAVFSIZLIKNI TA’MINLASH VA AXBOROT TEXNOLOGIYALARI SOHASIDAGI JINOYATLARGA QARSHI KURASHISHNI TAKOMILLASHTIRISH ISTIQBOLLARI

RESPUBLIKA ILMIY-AMALIY KONFERENSIYASI MATERIALLAR TO‘PLAMI

TOSHKENT
2023

AXBOROT TEXNOLOGIYALARI KAFEDRASI

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ
ИЧКИ ИШЛАР ВАЗИРЛИГИ
АКАДЕМИЯСИ

КИБЕРХАВФСИЗЛИКНИ ТАЪМИНЛАШ ВА АХБОРОТ ТЕХНОЛОГИЯЛАРИ СОҲАСИДАГИ ЖИНОЯТЛАРГА ҚАРШИ КУРАШИШНИ ТАКОМИЛЛАШТИРИШ ИСТИҚБОЛЛАРИ

Республика илмий-амалий конференция
материаллар тўплами

(22 декабрь 2023 йил)

ТОШКЕНТ – 2023

УДК 004(575.1)(082)

Ўзбекистон Республикаси ИИВ Академиясининг
Ўқув-услубий кенгашида маъқулланган

Маъсул муҳаррир:
А.Ф. Исақов

Тақризчилар:
Ўзбекистон Республикаси ИИВ Академияси Ахборот технологиялари кафедраси в.б., ф.-м.ф.н. А.А. Иминов, ю.ф.д. (DSc), проф. А.А. Матчанов.

Таҳрир ҳайъати:
А.А. Иминов, Б.Қ. Эргашев, И.М. Каримов.

Нашрга тайёрловчи:
М.Э. Камалов, Р.Х. Махамадов, С.З. Абдуазимов, А.У. Алиев, Х.З. Мухаммаджонов.

К 38 Киберхавфсизликни таъминлаш ва ахборот технологиялари соҳасидаги жиноятларга қарши курашишни такомиллаштириш истиқболлари Республика илмий-амалий конференция материаллар тўплами. 22 декабрь 2023 йил. Масъул муҳарир: А.Ф. Исақов. Ўзбекистон Республикаси ИИВ Академияси, 2023.- 427 б.

Ушбу мақолалар тўпламида ҳуқуқни муҳофаза қилувчи органларининг кибермаконда содир этилаётган жиноятларни олдини олиш, аниқлаш, бартараф этиш ва фош қилиш борасидаги фаолиятидаги мавжуд муаммоларни таҳлили, ахборот-коммуникация технологиялари соҳасидаги жиноятларга қарши курашда қўлланилаётган аппарат ва дастурий воситаларининг ўзаро алоқадорлиги, уларнинг ўзига хос жиҳатлари ҳамда ҳозирги ҳолати, ахборот-коммуникация технологиялари соҳасидаги жиноятларни аниқлаш, таснифлаш ва исботлаш, уларга қарши кураш йўналиши бўйича миллий илғор тажрибани ўрганиш ҳамда таҳлил қилиш масалалари ёритилган.

Мақолалар турдош олий таълим муассасаларининг профессор-ўқитувчилари, тадқиқотчилар ва амалиёт ходимлари, мустақил изланувчилар, тингловчи, курсант ва талабаларга мўлжалланган.

©Ўзбекистон Республикаси ИИВ Академияси, 2023

МУНДАРИЖА

ТУРАХОДЖАЕВ Н.С. КИБЕРХАВФСИЗЛИКНИ ТАЪМИНЛАШ ВА АХБОРОТ ТЕХНОЛОГИЯЛАРИ СОҲАСИДАГИ ЖИНОЯТЛАРГА ҚАРШИ КУРАШИШНИ ТАШКИЛ ЭТИШ МАСАЛАЛАРИ……..**1**

ВАЛИУЛИН А. Ш. КИБЕРПРЕСТУПЛЕНИЯ В СЕТИ DARKNET КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ……..**7**

ИМИНОВ А.А. ПРОБЛЕМЫ И ПУТИ ИХ РЕШЕНИЯ ПОДГОТОВКИ КАДРОВ ПО ОБСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ В АКАДЕМИИ МВД РЕСПУБЛИКИ УЗБЕКИСТАН……....**13**

ХАМРАҚУЛОВ У.Ш. КИБЕРЗЎРАВОНЛИК - ВИРТУАЛ ОЛАМДАГИ РИВОЖЛАНАЁТГАН ЖИНОЯТ СИФАТИДА…….....**18**

КУПРИЯНОВА И.М. ВИДЫ КИБЕРПРЕСТУПЛЕНИЙ И СПОСОБЫ БОРЬБЫ С НИМИ ……...……...……....**21**

МУХАММЕДОВ Ф.Н. INTERNETDAGI FIRIBGARLIK JINOYATLARI VA UNING XUSUSIYATLARI……...…..**25**

УЛУҒБЕКОВ А.А. ВИКТИМИЗАЦИИ ЖЕРТВ КИБЕРПРЕСТУПЛЕНИЙ…..……....**29**

МАРДИЕВ Ш.Ғ. АХБОРОТ ТЕХНОЛОГИЯЛАРИ СОҲАСИДА ИЛМИЙ - ТЕХНИКАВИЙ ИННОВАЦИЯДАН САМАРАЛИ ФОЙДАЛАНИШ ХУСУСИЯТЛАРИ…….……..**33**

КАМАЛОВ М.Э. КИБЕРМАКОНДА АХБОРОТ ХАОСИНИ ОЛДИНИ ОЛИШ……..…….…..**41**

АТАХАНОВ Б.Б., ФИВГХАМИДОВ М.У. ПРЕСТУПНОСТЬ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИИ, ВИДЫ И ПРИМЕРЫ МЕТОДОВ РЕШЕНИЕ……..…....**47**

РАИМОВ Н.Қ., ЭЎРМОНОВ Б.Б. PROSPECTS FOR IMPROVING CYBERSECURITY AND COMBATING CRIME IN THE FIELD OF INFORMATION TECHNOLOGY...……...**53**

БАБАДЖАНОВ С.С., ТЎРАЕВ Б.Т. ҲАРБИЙ ТАЪЛИМ МУАССАСАЛАРИ КУРСАНТЛАРИНИНГ МЕДИАХАВФСИЗЛИК КОМПЕТЕНТЛИГИ ВА УНИНГ МАЗМУНИ……..……...**58**

ШИХОВ Б.А. АППАРАТ-ДАСТУРИЙ ҚУРИЛМАЛАР АСОСИДА УЧУВЧИСИЗ УЧИШ АППАРАТЛАРИНИНГ МАЪЛУМОТЛАРНИ ҲИМОЯЛАШ…….....**63**

ХАМРАЕВА Г.Р. KIBERJINOYATCHILIKKA QARSHI KURASHDA AQSH VA O‘ZBEKISTON DAVLATLARINING QIYOSIY TAHLILI…….....**70**

МУСАЕВ А.И. MESSENDJERLARDA KALITLARNI XAVFSIZ ALMASHISH ALGORITMLARI……..…**78**

ХАМРОЕВ У.Р. KIBERXAVFSIZLIKNI TA’MINLASHDA STRATEGIK CHORALARNING O‘RNI VA AHAMIYATI……....**82**

САЙФУЛЛАЕВ Ш.Б. KORPORATIV TARMOQDA VIRUSGA QARSHI HIMOYAGA QO‘YILADIGAN TALABLAR.....**89**

МАВЛЯНОВ М.А. INTERNET TARMOG‘IDAN EKSTREMIZM VA TERRORIZM MAQSADLARIDA FOYDALANISHGA QARSHI KURASHISHNING AYRIM MASALALARI……...……....**93**

ШИХОВ Б.А. КИБЕРЖИНОЯТЛАР ВА УЛАРНИНГ КЕЛИБ ЧИҚИШИ……..……..**97**

ОТАЕВ Ў.М. КИБЕРМАКОНДА СОДИР ЭТИЛАЁТГАН ҲУҚУҚБУЗАРЛИКЛАР..……...**101**

БЕЙСЕНОВ К.С. КИБЕРХАВФСИЗЛИКНИ ТАЪМИНЛАШ ДАВР ТАЛАБИ……...**105**

Валиулин Артур Шавкатович,

Специалист центра кибербезопасности

КИБЕРПРЕСТУПЛЕНИЯ В СЕТИ DARKNET КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ УЗБЕКИСТАН

В настоящее время в мире особое внимание уделяется разработке и совершенствованию информационной безопасности, так как при нынешнем стремительном развитии информационной среды наряду с положительными аспектами наблюдается значительный рост киберпреступности. При этом все большую озабоченность у правоохранительных органов многих зарубежных странах, а также структурных подразделений международных организаций, вызывает противоправная деятельность в теневом пространстве Интернета в т.н. сети Darknet. Согласно ежегодного отчета Международного союза электросвязи ООН «Глобальный индекс по кибербезопасности 2020» киберпреступность становится инструментом осуществления противоправных деяний, так в 2020 году в США совершено 792 тыс. киберпреступлений что на 69 % больше чем в 2019 г., ущерб от которых превысил 4,2 млрд. долларов, аналогично в России число киберпреступлений увеличилось за 2020 год на 94 % составив 510 тыс. киберпреступлений 1.

При этом по данным Генеральной прокуроры Узбекистана за последние три года число киберпреступлений в Узбекистане выросло почти в 25 раз. Данное также подтверждается данными ГУВД столицы, согласно которым количество киберпреступлений, зарегистрированных в Ташкенте, за 2022 год увеличилось в 1,9 раза, так в 2020 году было выявлено 106 преступлений в сфере информационных технологий, в 2021 году - 2281, а в 2022 году - 4332.

Одновременно наблюдается увеличение количества пользователей сети Darknet на территории Узбекистана со 1000 ежедневных пользователей в

[1] Отчет ООН «Глобальный индекс кибербезопасности 2020»// Global Cybersecurity Index 2020. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-20-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

январе 2021 года до 100 тыс. в настоящее время[2].

В настоящее время 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 Net.

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 (рисунок 1.).

Рисунок 1. Образное представление всемирного виртуального пространства

При этом немалую озабоченность вызывают киберпреступления в сети Darknet, где имеются сведения о методах взлома информационных систем, осуществляется распространение персональных данных и вредоносных программ, предоставляется хостинг, а также ресурсы для обмена запрещенным контентом.

Указанные угрозы способствующие киберпреступлениям в сети Darknet были разделены на 3 вида угроз таких как: взлом информационных ресурсов и изготовление вредоносных программ; незаконное распространение персональных данных; предоставление хостинга и обмен запрещенным контентом.

Анализ Darknet сайтов, несущих угрозы кибербезопасности Республики Узбекистан, указывает на значительное количество ресурсов предлагающих услуги взлома информационных ресурсов и изготовления вредоносных программ.

В частности, согласно результатам исследования международной

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

компании по разработке программного обеспечения в области информационной безопасности «Positive Technologies», на сегодняшний день рынок преступных киберуслуг на специальных профильных сайтах обеспечивает всего 30% поступающих заказов. При исследовании специалисты компании проанализировали более 10000 объявлений по поиску или предложению услуг по разработке хакерских программных обеспечений на 25-ти наиболее популярных сайтах в Darknet. На фоне роста курса различных криптовалют наиболее популярной категорией вредоносного программного обеспечения становятся программы для скрытого майнинга - его доля среди предлагаемого к продаже софта достигает 20%. При этом на такое программное обеспечение приходится почти четверть кибератак. За ними следуют различные хакерские инструменты (19%), вредоносный софт для создания сетей зараженных компьютеров (14%) и вирусы-вымогатели (12%)[3].

Наибольшее количество хакерских услуг предлагаются в виртуальных магазинах, размещенных на торговых площадках KRAKEN (бывшая HYDRA), Grey Market и Samara Marketи др. При этом в сети Darknet имеются множество форумов, где хакерами обсуждаются методы взлома информационных ресурсов, выявления в них уязвимостей, по индивидуальным заказам изготавливаются вредоносные программы способные внедрится в систему и на постоянной основе отправлять новые материалы и т.н.

Примером тому служит ресурс Picochan позволяющий после анонимной регистрации заказывать или предоставлять услуги по взлому информационных ресурсов.

Сайт «Hackers collective» предлагает широкий спектр услуг. Хакеры этого ресурса подразделяются на 3 класса, которые определяются многолетним опытом и мастерством. Услуги хакеров класса «С» колеблется от 500 до 1500 долларов США. Они выполняют задания по взлому «Facebook», «Twitter» и др. социальных сетей, учетных записей электронной почты и рассылке спамов.

Нередко хакеры объединяются в отдельные группы и организованно осуществляют взлом или атаку на информационный ресурс. К примеру ресурс «Pundit Hackers Group» состоит их групп высококвалифицированных программистов, способных проводить кибератаки любой сложности. В их числе получение доступа к паролю, восстановление удаленных учетных записей, а также удаление учетных записей в социальных сетях, взлом сайта

[3]Александров А. Г., Сафронов А. А. Использование сети Даркнет при подготовке и совершении преступлений // Вестник Санкт-Петербургского университета МВД России. – 2021. – № 1. – С. 156–160.

вне зависимости от сложности платформ сайта. Аналогично ему группа «Hacker for Hire» оказывает услуги по взлому аккаунтов в социальных сетях, компьютерному шпионажу и слежке, удалению ссылок, проверке данных, кибер-преследованию, а также кибер-вымогательству.

Также сообщество хакеров «HackersBay» (рисунок 2.) предлагает услуги анонимного взлома сайтов, персональных компьютеров, сотовых телефонов, аккаунтов в социальных сетях, электронных почт и организации DDoS-атак[4].

Рисунок 2. Сообщество хакеров «HackersBay»

Одной из актуальных угроз, исходящих из сети Darknet остается незаконное распространение персональных данных[5].

Как показывает анализ контента сайтов Darknet, в последнее время резко выросло количество ресурсов, специализирующихся на торговле конфиденциальной информацией. Основную часть отмеченной информации составляют персональные данные, платежные сведения, информация финансово-кредитной и страховой сферы, промышленных и транспортных систем, компаний отрасли торговли и высокотехнологичного бизнеса.

При этом за последнее время более чем в 27 раз увеличился объем утечек персональных данных и платежной информации, скомпрометированных в результате неосторожности или неправомерных действий персонала финансового сегмента, страховых компаний, а также в результате активности внешних злоумышленников.

Как показывают результаты анализа сайтов Darknet, на торговой площадке Dream Market в Darknet выставлены на продажу 617 млн. учетных записей, похищенных из 16 взломанных сайтов.

Материалы и базы данных зачастую продаются оптом или в розницу в сети Darknet. В качестве примера данной деятельности в Узбекистане можно привести виртуальный магазин Better Call Saur (рисунок 3.), функционировавший до сентября 2022 года на торговой площадке HIDRA, предоставляющий услугу по получению установочных данных наших

[4]Николаев К. Анализ работы сети с луковой маршрутизацией в рамках поиска скрытых сервисов по продаже и покупке вредоносного программного кода для взлома программного обеспечения воздушного судна. // 2018 год

[5]Мазур А.А. Актуальные проблемы предупреждения преступности в социальной сети Даркнет // Вестник Российского института кооперации. - Москва, 2018. - № 3. - С. 125-129.

граждан по номеру телефона т.н. «Пробив номера».

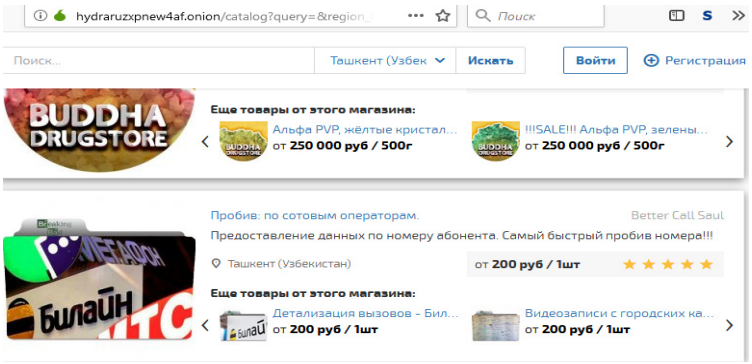

Рисунок 3. Виртуальный магазин BetterCallSaur

По мнению специалистов, в сфере кибербезопасности, существуют несколько методов кражи или раскрытия личных данных, которые затем продаются через сайты Darknet. К таким методам относятся обычная кража личных данных, инсайдерская кража, скимминг и кардинг финансовой карты, взлом базы данных больших компаний, фишинг (на основе электронной почты), SMS-shing (на основе текста) и Vishing (на основе голоса).

Одним из ресурсов с материалами конфиденциального содержания является сайт CMARKET где продается большой объем персональных данных из европейских государств содержащие ФИО, идентификационные номера, домашний адрес, биометрические персональные данные, номер социального страхования, данные кредитной карты и др сведения.

Следующим видом угроз, исходящим от сети Darknet, является предоставление хостинга в сети Darknet и обмен запрещенным контентом. В частности, в своей противоправной деятельности деструктивные элементы используя анонимность сети Darknet размещают свои сайты на отдельных площадках данной сети, а также посредством отдельных почтовых сервисов осуществляют обмен запрещенным контентом, в том числе террористического и иного содержания.

В качестве примера можно привести ресурс The Best Deep Web Hosting (рисунок 4.) предоставляющий услуги хостинга и почтового клиента.

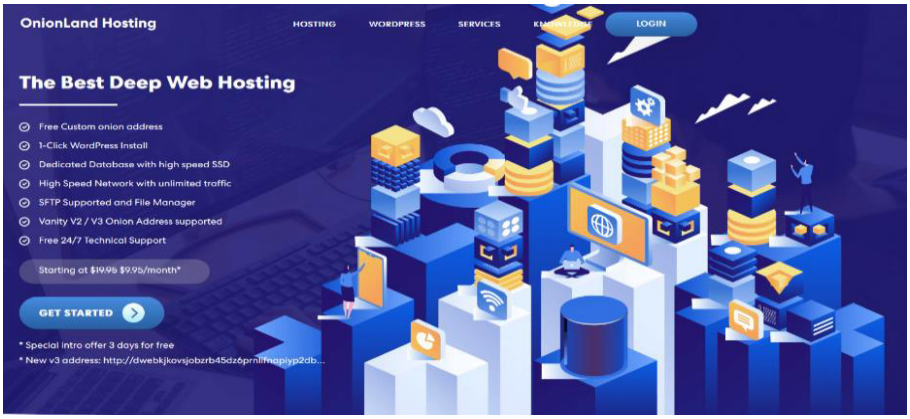

Рисунок 4. Ресурс The Best Deep Web Hosting

Вместе с тем сайт BlackHost предлагает пользователям несколько сервисов, позволяющих анонимно обмениваться файлами, электронной почтой, проводить шифрование данных. При этом ресурс TorFront представляет сервис по продаже ONION-доменов.

В данном исследовании освещены всего 3 угрозы исходящие от сети Darknet и способствующие росту киберпреступлений. При этом в рассматриваемой сети имеется множество угроз таких как распространение наркотиков, оружия и взрывчатых веществ, пропаганда терроризма, суицида, продажа поддельных документов и купюр, и другие угрозы в основном направленные на молодёжь. В ходе анализа угроз исходящих от теневого пространства интернета выявлено что, большинство ресурсов данной сети имеют элементы разносторонней деструктивной деятельности, несущей угрозу информационной безопасности Республики Узбекистан.

Активизация информационной безопасности страны, идет в унисон с одним из семи приоритетных направлений развития Нового Узбекистана в 2022-2026 годах утвержденным Указом Президента Республики Узбекистан, где определены задачи по обеспечению информационной безопасности, в том числе «…Повышение культуры пользования граждан информационно-коммуникационными средствами. Предотвращение нарушения права неприкосновенности связанного с опубликованием в сети Интернет личных и конфиденциальных данных. Создание системы предупреждения киберпреступности»[6]. С учетом изложенного в рамках межведомственного сотрудничества в борьбе с противоправной деятельностью в сети Darknet предлагается продолжить совместную работу по выявлению информационных ресурсов данной сети, определению специфик противоправной деятельности субъектов в теневом пространстве интернета, обмену опытом в ее выявлении и пресечении, а также осуществлять анализ основополагающих нормативно-правовых документов в области информационной безопасности с целью их своевременной корректировки.

[6] Указ Президента Республики Узбекистан № УП-60 от 28 января 2022г. «О Стратегии развития Нового Узбекистана на 2022-2026 годы» // База данных нормативно-правовой информации Norma