Л.Н. Гумилев атындағы Еуразия ұлттық университетінің ХАБАРШЫСЫ.
ISSN: 2616-6887. eISSN: 2617-605X
САЯСИ ҒЫЛЫМДАР/ POLITICAL SCIENCE / ПОЛИТИЧЕСКИЕ НАУКИ

МРНТИ: 11.93.29 https://doi.org//10.32523/2616-6887/2024-148-3-46-60
Научная статья

Вопросы кибербезопасности в решении глобальных задач ООН по борьбе с терроризмом

Р.Е. Садыкова

Eurasian Communications Centre, Астана, Казахстан

(E-mail: rizvana7@gmail.com)

Аннотация. На сегодняшний день угрозы кибербезопасности являются одной из основных проблем, с которыми сталкиваются все страны. Киберпространство играет важную роль в нашей современной жизни, объединяя людей и сообщества по всему миру, обеспечивая им возможность социализации и самоорганизации.

Данная статья освещает основные виды кибератак и угроз, а также предлагаются методы их предотвращения. Рассматриваются различные типы киберпреступлений, а также необходимые действия для борьбы с кибертерроризмом. Киберпреступники активно используют различные методы и техники для осуществления кибератак, включая несанкционированный доступ к системам, кражу личной информации, финансовые мошенничества и распространение вредоносного программного обеспечения. Кибертерроризм также представляет опасность, поскольку кибератаки могут быть использованы для создания хаоса и нарушения функционирования критически важных инфраструктур, таких, как государственные институты, системы здравоохранения, энергетики и так далее. Для обеспечения кибербезопасности необходимо сотрудничество как на государственном, так и на международном уровне. На международном уровне важно установить диалог между различными странами и международными организациями, такими, как ООН, Европейский союз, НАТО и другие. Это позволит согласовывать стратегии, координировать меры по предотвращению и реагированию на кибератаки.

Ключевые слова: киберпространство, угрозы кибербезопасности, кибертерроризм, сотрудничество по кибербезопасности.

Поступила: 24.04.2024; Принята: 16.09.2024; Доступна онлайн: 25.09.2024

Введение

Понятие «кибербезопасности» имеет несколько толкований. Одно из таких толкований, предложенное исследователем Д.Б. Дубининой, описывает кибербезопасность как комплекс мер по защите систем, сетей и программных приложений от цифровых атак, нацеленных на получение доступа к конфиденциальной информации, ее изменение, уничтожение или вымогательство денег у пользователей [1].

Другое толкование, предложенное Н.А. Моисеевой, связано со знаниями и умениями в области оценки рисков социальной инженерии при работе в цифровом пространстве, организации безопасности персональных данных, а также с осознанием негативного влияния цифровых устройств и гаджетов на окружающую среду, а также на физическое и психическое здоровье человека [2].

В международном стандарте ISO/IEC 27032:2012 [3] кибербезопасность определяется как свойство защищенности активов от угроз конфиденциальности, целостности и доступности в киберпространстве. А в ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 [4] более широкое определение кибербезопасности дается как действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли или повреждения критических систем или информационных объектов. Кибербезопасность включает в себя понятия идентификации, аутентификации, отслеживаемости, авторизации, доступности и приватности [5].

В международных стандартах существует несколько определений понятия "кибератака", которые охватывают различные аспекты данного понятия. Ниже приведены некоторые из них:

В ISO/IEC 27032:2012 [3] "Кибератака" определяется как "любое действие, направленное на получение несанкционированного доступа к информации или на ее изменение, уничтожение или блокирование, выполняемое при помощи средств вычислительной техники или коммуникационной технологии".

В Национальном институте стандартов и технологий США (NIST) кибератака определяется как "любое нежелательное событие или действие, направленное на компьютерную систему или сеть, которое нарушает конфиденциальность, целостность или доступность компьютерной системы или сети".

В ГОСТ Р ИСО/МЭК 27005-2017 [6] "Кибератака" определяется как "любое нежелательное событие, вызывающее нарушение конфиденциальности, целостности или доступности информации, хранимой, обрабатываемой или передаваемой в информационной системе".

Согласно исследованиям, проводимым различными организациями, средний пользователь проводит в интернете более 6 часов в день. Однако плотное взаимодействие с киберпространством несет с собой определенные риски для пользователей. Киберпреступники используют различные методы, чтобы получить доступ к личной информации и деньгам пользователей. Поэтому существует необходимость в обеспечении безопасности в киберпространстве. Специалисты по кибербезопасности

работают над созданием различных методов и технологий для защиты пользователей от киберугроз. Они также разрабатывают стандарты и рекомендации для организаций и государств, чтобы обеспечить безопасность в сети. И это находит свое отражение в ряде стандартов и нормативно-правовых документов, таких, как ISO/IEC 27032:2012 [7], NIST CSF [8], ISO/IEC 27001[9], стандарт IEC 62443 [10]. Все эти документы помогают улучшить защиту персональных данных и информации от кибер-угроз [11].

Методы исследования

Эта статья посвящена изучению и анализу некоторых аспектов борьбы с терроризмом в условиях глобализации. В контексте развития новых форм терроризма и прогресса в области технологий и киберпространства, рассматриваются исторические аспекты и проблемы.

В работе проводится обзор истории и условий борьбы с терроризмом с учетом глобализации и развития киберпространства и новых технологий. Особое внимание уделяется анализу успешных практик и деятельности организаций Организации Объединенных Наций (ООН) в области активизации регионального сотрудничества. Учитываются вопросы, связанные с использованием киберпространства и новых технологий террористическими группировками.

В работе авторы опираются на различные официальные документы, заключения и заявления, включая опыт и мнения общественных деятелей и межгосударственных структурных органов. Для поддержки исследования использовались различные источники, включая официальные веб-сайты и базы данных.

Таким образом, данная статья представляет собой аналитическое исследование, основанное на исторических фактах, анализе официальных документов и опыте международных организаций. Она призвана рассмотреть современные вызовы в борьбе с терроризмом и исследовать возможности усиления регионального сотрудничества с учетом глобализации и развития киберпространства и новых технологий.

Международный союз электросвязи (МСЭ) создал Глобальную программу кибербезопасности с целью укрепления доверия и безопасности в информационном обществе. В рамках этой программы МСЭ определил пять ключевых стратегических принципов: правовые, технические и организационные меры, развитие потенциала и международное сотрудничество (Рисунок 1).

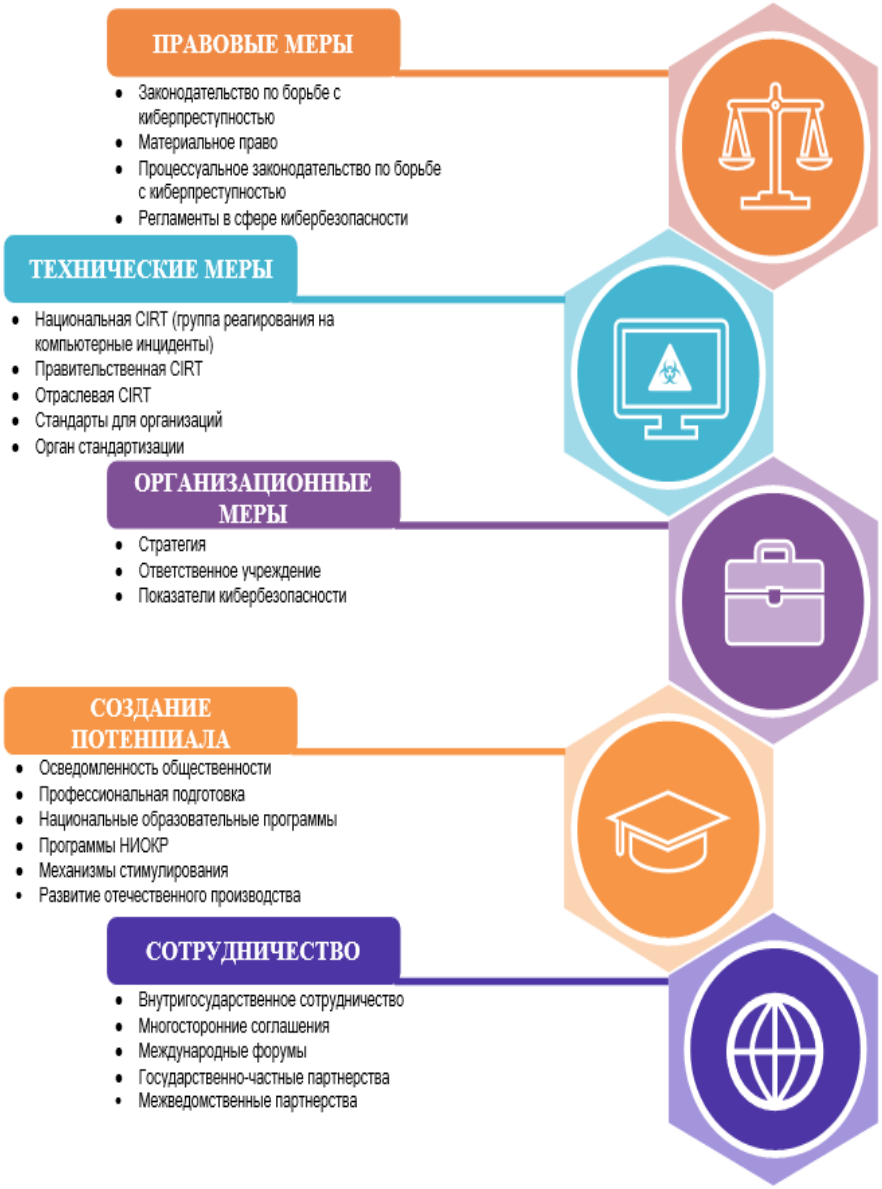

Рисунок 1. Пять стратегических принципов

У Контртеррористического управления ООН есть несколько инициатив в области новых технологий. Программа «Кибербезопасность и новые технологии» направлена на расширение возможностей государств-членов и частных организаций по предотвращению и смягчению последствий неправомерного использования технологических разработок террористами и воинствующими экстремистами. Это включает в себя противодействие угрозе кибератак, совершаемых террористами на критически важную инфраструктуру, а также развитие использования социальных сетей для сбора информации из открытых источников и цифровых доказательств для противодействия онлайн-терроризму и насильственному экстремизму при соблюдении прав человека. Программа также предоставила экспертную оценку международным форумам по

использованию беспилотных авиационных систем (БАС) террористами и будет разрабатывать дальнейшие программы в этой области. Проект также направлен на смягчение воздействия, а также восстановление целевых систем в случае возникновения таких атак.

В ходе шестого обзора Глобальной контртеррористической стратегии (A/RES/72/284) государства-члены выразили озабоченность по поводу более широкого использования террористами информационно-коммуникационных технологий (ИКТ), в частности, интернета и других средств массовой информации, а также использование таких технологий для совершения, подстрекательства, вербовки, финансирования или планирования террористических актов. Государства-члены далее отметили важность сотрудничества между заинтересованными сторонами в осуществлении Стратегии, в том числе между государствами-членами, международными, региональными и субрегиональными организациями, частным сектором и гражданским обществом.

В резолюции 2341 (2017) Совет Безопасности призывает государства-члены «устанавливать или укреплять национальные, региональные и международные партнерства с заинтересованными сторонами, как государственными, так и частными, в зависимости от обстоятельств, для обмена информацией и опытом в целях предотвращения, защиты, смягчения последствий расследовать, реагировать и устранять ущерб от террористических атак на объекты критической инфраструктуры, в том числе путем совместного обучения, а также использования или создания соответствующих сетей связи или оповещения о чрезвычайных ситуациях».

В 2021 году Глобальная программа UNCCT по кибербезопасности и новым технологиям запустила специализированную масштабную годовую поддержку Буркина-Фасо в области кибербезопасности и цифровой криминалистики и укрепила потенциал правоохранительных органов страны по сбору цифровых доказательств для судебного преследования и судебного разбирательства по делам о террористических преступлениях.

Программа также расширила навыки и возможности Буркина-Фасо, Бангладеш, Мальдивских Островов, Малайзии и Филиппин для применения методов расследования для получения и анализа цифровых доказательств из зашифрованных и открытых источников, необходимых для привлечения террористов к ответственности, при полном соблюдении права человека и верховенство права. В рамках стратегического взаимодействия КТЦ ООН с НАУСС Программа организовала совместное обучение 49 сотрудников системы уголовного правосудия из Западной Африки и арабских государств в учебных центрах НАУСС, что не только повысило их навыки в области цифровой криминалистики, но и укрепило региональное сотрудничество и участие в противодействие терроризму. Все участники признали, что обучение КТЦ ООН улучшило их понимание влияния сбора и анализа цифровых доказательств на права человека и того, как снизить риски для прав человека в их следственной работе [12].

Типы угроз и атак

В киберсреде существует множество различных типов угроз и атак, которые могут привести к нарушению кибербезопасности. Ниже представлен краткий обзор на наиболее распространенные типы угроз и атак (Рисунок 2).

Рисунок 2. Наиболее часто встречающиеся угрозы в области кибербезопасности

Вирусы и другое вредоносное программное обеспечение распространяются через электронную почту, загрузки из интернета и т.д. Кроме того, они могут быть использованы кибертеррористами для нанесения ущерба целевым системам и сетям, а также для сбора конфиденциальной информации. Кибертеррористы могут создавать и распространять различные типы вредоносных программ, таких, как вирусы, троянские программы и шпионское ПО, которые вызывают различные виды угроз, включая кражу личных данных, блокировку компьютеров и сетей, а также удаление или изменение важной информации.

Фишинг, фарминг и другие атаки на персональные данные являются серьезной угрозой кибербезопасности. Эти атаки могут использоваться в кибертерроризме для получения конфиденциальной информации, такой, как пароли, номера кредитных карт и другие личные данные. Кибертеррористы могут использовать эти данные для кражи денег или для дискредитации определенных личностей или организаций. Например, фишинг-атаки проводятся путем отправки злоумышленниками электронных писем

или сообщений, которые выглядят как легитимные, но на самом деле предназначены для получения конфиденциальной информации. Фарминг-атаки, с другой стороны, используют поддельные веб-сайты, чтобы собирать информацию от пользователей, которые вводят свои логины и пароли на этих сайтах [13], [14].

Манипуляция людьми с помощью социальной инженерии становится все более значимой угрозой для виртуальных сообществ и эффективным средством для атак на информационные системы. Социальная инженерия также является важной составляющей в кибертерроризме, который представляет собой использование киберпространства для организации террористических актов. Кибертеррористы могут использовать социальную инженерию для манипулирования людьми, чтобы заставить их поверить в ложные идеологии, участвовать в террористических деятельностях или распространять террористическую пропаганду.

Например, кибертеррористы могут использовать социальную инженерию, чтобы маскировать свои атаки под легитимные коммуникации и запросы на информацию, чтобы получить доступ к защищенным системам и конфиденциальным данным. Они также могут использовать социальную инженерию, чтобы распространять вирусы, троянские программы и другое вредоносное программное обеспечение с помощью фишинговых атак, мошеннических сайтов и других методов.

В области кибербезопасности социальная инженерия относится к манипулированию людьми с целью разглашения конфиденциальной информации или выполнения определенных действий, которые могут быть полезны злоумышленнику. Самое опасное в социальной инженерии заключается в том, что для ее эффективного применения не обязательно обладать высоким уровнем технической подготовки. Она базируется на понимании основных принципов человеческой психологии.

Управление безопасностью информационных систем должно включать как технологические, так и управленческие меры, включая контроль за поведением сотрудников, имеющих доступ к конфиденциальной информации [15].

DDoS-атаки: это атаки, которые осуществляются путем создания огромного количества запросов на определенный сервер или сайт, что может привести к его перегрузке и выходу из строя. DDoS-атаки, или атаки на отказ службы, могут быть использованы в кибертерроризме для отключения важных систем и сетей. Кибертеррористы могут использовать ботнеты - сети зараженных компьютеров, чтобы отправлять большое количество запросов к серверам, перегружая их и делая недоступными для пользователей. Это может нанести ущерб критическим системам, таким, как банковские системы, системы энергоснабжения, системы управления транспортом и т.д.

Изначально ботнеты разрабатывались для выполнения определенных задач внутри группы. Он определяется как сеть или группа устройств, подключенных к одной сети для выполнения задачи. Но теперь это используется злоумышленниками и хакерами, которые пытаются получить доступ к сети и внедрить любой вредоносный код или вредоносное ПО, чтобы нарушить ее работу. Атаки ботнетов обычно осуществляются против крупных предприятий и организаций из-за их огромного доступа к данным. Благодаря этой атаке хакеры могут контролировать множество устройств и скомпрометировать их в своих целях [14].

Кибершпионаж: это мониторинг и сбор конфиденциальной информации о компаниях, правительствах или других организациях. Кибершпионаж – это вид кибератаки, при которой злоумышленник получает доступ к конфиденциальной информации, находящейся на компьютерах, серверах или сетях, с целью использовать ее для коммерческого или политического выгоды. Цели кибершпионажа могут варьироваться от кражи интеллектуальной собственности до получения государственных тайн.

Программа-вымогатель – это программа для шифрования файлов, которая использует уникальный надежный алгоритм шифрования файлов в целевой системе. Авторы программ-вымогателей пользуются этим и требуют от жертв значительную сумму выкупа за предоставление кода дешифрования или расшифровку данных. Но такие атаки не имеют гарантии восстановления данных даже после уплаты выкупа.

Кроме того, в последние годы появился новый тип угрозы – кибертерроризм. Кибертерроризм – это использование компьютерных технологий и киберпространства для осуществления террористических действий, например, для остановки работы критически важных систем или для получения конфиденциальной информации, то есть кибертеррористы используют технологии информационных систем, чтобы дестабилизировать государства и организации, вызвать панику и страх в обществе и проводить кибератаки на государственные институты. В связи с этим в последнее время государства активно занимаются разработкой стратегий и мер для борьбы с кибертерроризмом, включая усиление кибербезопасности критически важных объектов и инфраструктуры.

Существует несколько основных видов киберугроз, которые могут нанести вред пользователям в киберпространстве. Среди них можно отметить кибербуллинг, который проявляется в форме целенаправленной травли, оскорблений и угроз с использованием современных средств коммуникации. Киберэкстремизм включает пропаганду экстремистских взглядов в киберпространстве. К другим видам киберугроз можно отнести угрозы для морали и нравственности, в том числе сцены жестокости, употребления алкоголя, наркотиков и.т.д. Кроме того, существует агрессивное информационное пространство, которое включает манипуляции сознанием и пропаганду от навязчивой рекламы товаров и услуг до навязывания политических взглядов. Все эти виды киберугроз могут нанести серьезный вред пользователям в киберпространстве, поэтому важно принимать меры по обеспечению кибербезопасности [4] [7] [16].

Методы защиты. Анализируя мнение ведущего аналитика отдела развития ООО «Доктор Веб» Вячеслава Медведева и других специалистов в этой сфере, можно прийти к выводу, что абсолютной защиты в киберсистеме не существует. Однако, пользуясь методами обеспечения защищенности, можно постараться сохранить свои данные и при этом спокойно использовать электронные ресурсы.

Несколько правил помогут поддерживать компьютерную безопасность на нужном уровне, такие, как установка антивирусной защиты и ее актуальное обновление, создание службы по управлению кибербезопасностью, использование оборудования, оснащенного защитой от киберугроз, резервное копирование информации, ограниченное использование социального пространства и обновление программ безопасности.

Проанализировав случаи нарушения компьютерной безопасности с использованием социальных сетей, можно сформулировать основные советы для безопасного пользования ими: придумывать разнообразные и усложненные пароли для защиты своих страниц, регулярно менять пароли в социальных сетях, быть особенно осторожными при открытии ссылок на сторонние сайты, не размещать конфиденциальную информацию на странице, ограничивать доступ сторонних лиц к личной информации и быть настороже при общении с незнакомцами, которые проявляют неподдельный интерес к личной жизни. Также следует избегать распространения и ввода персональных данных на незнакомых сайтах, не открывать подозрительную почту и не переходить по подозрительным ссылкам. Кроме того, можно использовать технологии фильтрации электронной почты, чтобы избежать фишинговых атак и определить правила, ограничивающие доступ к информации [12], [17].

Кибербезопасность как средство противодействия терроризму играет критически важную роль в защите от кибератак и киберпреступлений, которые могут быть использованы террористами для дестабилизации и нарушения нормального функционирования государственных и частных систем.

Использование компьютерных сетевых устройств террористами для саботажа критически важных национальных инфраструктур, таких, как энергетические, транспортные системы, водоснабжение, государственные учреждения, здравоохранение или связь, вызывает все большую озабоченность у государств-членов Организации Объединенных Наций. Несколько террористических организаций, в том числе «Аль-Каида» и ИГИЛ/Даиш, выразили намерение создать наступательные кибервозможности, которые позволили бы им проводить потенциально разрушительные атаки издалека. Совершенно очевидно, что государства-члены нуждаются в обеспечении безопасности и устойчивости к таким нападениям, а также в способности смягчать их последствия, восстанавливать их в случае их возникновения, а также привлекать виновных к ответственности.

Исследования показали, что такие явления, как вербовка террористами и распространение воинствующего экстремистского контента по всему миру, стали возможными благодаря глобальному охвату интернета. Исследования также показали, что «слава ИГИЛ, которая привлекла внимание всего мира как самая жестокая исламистская террористическая группировка нашего времени, была бы невозможна без интернета и широкополосной связи […]. Тот факт, что ИГИЛ удалось захватить первые страницы крупнейших мировых новостных агентств, был преднамеренным».

За последнее десятилетие важные разработки в области цифровых технологий приобрели все возрастающую роль в прогрессе мировой экономики и общества, в том числе 1) аналитика больших данных, 2) искусственный интеллект, 3) существенное увеличение вычислительной мощности, 4) кибербезопасность и шифрование, 5) мобильные сети 5G, 6) блокчейн и 7) взаимосвязанные устройства и интернет вещей (IoT). Хотя преимущества этих технологий неоспоримы, существует риск того, что они также могут быть использованы со злым умыслом для распространения экстремистских нарративов и осуществления кибератак террористами. Поэтому необходимо действовать упреждающе и разрабатывать решения, охватывающие эти технологии, чтобы противодействовать их злонамеренному использованию террористами [18].

Угрозы в киберпространстве не ограничиваются только одной страной, а могут возникнуть в любой точке мира и нанести вред не только одной организации или государству, но и всему международному сообществу.

В этой связи международное сотрудничество в области кибербезопасности становится все более важным. Международное сотрудничество в области кибербезопасности включает в себя обмен информацией и опытом, координацию действий, разработку стандартов и правил поведения в киберпространстве, а также совместные усилия по предотвращению киберугроз и реагированию на них.

Также международное сотрудничество в области кибербезопасности позволяет обмениваться информацией и опытом в области киберзащиты и киберпреступности. Также международные организации могут создавать стандарты и рекомендации в области кибербезопасности, которые могут быть приняты и использованы различными странами.

Существует множество организаций и инициатив, направленных на укрепление международного сотрудничества в области кибербезопасности, таких, как Международный союз электросвязи (ITU), Организация экономического сотрудничества и развития (ОЭСР), Форум по кибербезопасности в рамках Всемирного экономического форума и др. Также государства могут заключать двусторонние и многосторонние соглашения по вопросам кибербезопасности.

Кроме того, необходимо проводить регулярные международные учения и тренировки для обучения специалистов в области кибербезопасности и повышения квалификации. Такие учения помогут разработать и уточнить процедуры реагирования на угрозы кибербезопасности и совершенствовать методы защиты информации.

В целом международное сотрудничество в области кибербезопасности является ключевым фактором в обеспечении безопасности в киберпространстве. Для защиты от кибератак и киберпреступлений, связанных с терроризмом, государства и частные компании должны принимать комплекс мер по повышению кибербезопасности. В частности, они должны усилить меры безопасности, такие, как двухфакторная аутентификация, шифрование, сетевые фильтры и многоуровневые защитные механизмы.

Однако необходимо учитывать, что кибербезопасность – это не только технические меры, но и обучение персонала. Государства и частные компании должны помнить, что обучение персонала является одним из важнейших аспектов обеспечения кибербезопасности в организации. Сотрудники организации могут быть неосведомленными о кибербезопасности или не понимать важность ее соблюдения, что может привести к ошибкам и нарушениям безопасности. Работники должны быть обучены распознаванию мошеннических попыток, использованию надежных паролей, работе с электронной почтой и другими инструментами, их безопасном использовании, а также соблюдению политик безопасности.

Кроме того, необходимо проводить регулярные проверки и аудиты, чтобы убедиться в том, что персонал соблюдает политики безопасности и использования информационных ресурсов организации. В целом обучение персонала должно быть неотъемлемой частью стратегии кибербезопасности организации.

Так как террористы могут использовать интернет для популяризации своих идей и рекрутинга новых членов, необходимо осуществлять мониторинг интернет-активности

и контроль за распространением террористической пропаганды и рекрутинга в интернете. Необходимо регулярно проводить анализ данных для выявления попыток психологического воздействия на пользователей интернета.

Для предотвращения таких влияний необходимо обеспечить доступность информации о рисках, связанных с подобными группировками, а также проводить профилактические мероприятия, направленные на предотвращение радикализации и экстремизма в сети.

Для повышения эффективности мер по кибербезопасности необходимо учитывать поведенческие особенности людей, которые могут стать жертвами кибербуллинга или попасть в сети под влияние религиозных сект, экстремистских организаций и т.д. Также важно создавать условия для помощи и поддержки людей, ставших жертвами кибернасилия. Для этого нужно организовывать кампании по информированию об киберугрозах, создавать условия для анонимной подачи жалоб на насилие в сети, а также обеспечивать юридическую помощь.

Наконец, необходимо организовывать образовательные курсы по кибербезопасности, в том числе дистанционные, чтобы повышать осведомленность и компетенцию в области кибербезопасности среди широкой публики, включая государственных служащих, бизнес-лидеров и обычных пользователей сети. Это поможет сформировать культуру безопасности в обществе и предотвратить потенциальные угрозы в области кибербезопасности [4].

Заключение

В современном обществе обеспечение кибербезопасности приобретает преимущественное значение в контексте решения глобальных задач Организации Объединенных Наций по борьбе с терроризмом. Национальная безопасность, общественная стабильность и экономическое благополучие тесно связаны с эффективной защитой информационных ресурсов. С увеличением влияния информационных технологий на нашу жизнь, угрозы кибербезопасности становятся не только разнообразными, но и более серьезными. Это влечет за собой постоянную необходимость усовершенствования методов и технологий защиты информационных систем и данных.

Информационное пространство, ставшее неотъемлемой частью жизни людей и организаций по всему миру, представляет собой ценную мишень для киберпреступников и кибертеррористов. Информационная война, разворачивающаяся в киберпространстве, может иметь серьезные последствия для национальной и общественной безопасности.

Кибербезопасность требует постоянного внимания и сотрудничества со стороны правительств, организаций и общественности. В этом контексте настоятельно важно укреплять международное сотрудничество в области кибербезопасности, разрабатывать инновационные технологии и методы защиты информационных систем и данных, а также повышать уровень информированности населения о возможных угрозах кибербезопасности и способах защиты личных данных.

Постоянное стремление к сотрудничеству и взаимодействию в области кибербезопасности может стать основой для создания устойчивого и надежного киберпространства, что важно для решения глобальных задач ООН по борьбе с терроризмом.

Список литературы

1. Дубинина Д.Б. Проблема медиабезопасности и кибербезопасности личности школьника и студента в современном информационном пространстве // Экология медиасреды: материалы IV открытой межвузовской научно-практической конференции. - 2019. – С.96-101.

2. Моисеева Н.А. Кибербезопасность как важный компонент цифровой грамотности поколения Z, Цифровизация и кибербезопасность: современная теория и практика // Сборник международной научно-практической конференции. - 2021. – С.191–196.

3.https://1cert.ru/novosti/iso-27032-2012-privatnost-v-eru-vsepronikayushchey-informatsii?-utm_referre [Электронный ресурс] (дата обращения: 24.04.2023).

4. Сети коммуникационные промышленные (Защищенность (кибербезопасность) сети и системы). – М.: Стандартинформ, 2014. – 80 с.

5. Путято М.М, Макарян А.С. Кибербезопасность как неотъемлемый атрибут многоуровневого защищенного киберпространства // CASPIAN JOURNAL: Control and High Technologies, №3 (51). - 2020. - С. 94-102.

6. https://www.tadviser.ru/index.php/ [Электронный ресурс] (дата обращения: 24.04.2023).

7. https://cyberleninka.ru/article/n/rukovodyaschie-ukazaniya-po-kiberbezopasnosti-v-kontekste-iso-27032/viewer [Электронный ресурс] (дата обращения: 24.04.2023).

8. https://learn.microsoft.com/ru-ru/compliance/regulatory/offering-nist-csf [Электронный ресурс] (дата обращения: 24.04.2023).

9. https://ru.wikipedia.org/wiki/ISO/IEC_27001 [Электронный ресурс] (дата обращения: 24.04.2023).

10. https://en.wikipedia.org/wiki/IEC_62443 [Электронный ресурс] (дата обращения: 24.04.2023).

11. Воскрекасенко О.А., Киреева А.А., Щелина Т.Т. Формирование культуры кибербезопасности в Системе профессиональной подготовки обучающихся колледжа как педагогическая проблема // Современные наукоемкие технологии, №10. -2022. - С.125-128.

12. Cybersecurity and New Technologies. Office of Counter-Terrorism. URL: https://www.un.org/counterterrorism/ru/cct/programme-projects/cybersecurity

13. Губенков А.О., Лукьянова В.В. Актуальные проблемы кибербезопасности в социальных сетях // Автономия личности, № 3(26). -2021. - С.46-53.

14. Маткаримов А., Бердиева Б., Ашырова М. Basics of Cyber Security and Its Need // Cognitio Rerum, №3. - 2023. - С.111-114.

15. Воробьева И.А., Сазонов А. Методы социальной инженерии в контексте кибербезопасности: информатика, вычислительная техника и управление // Естественные и технические науки, №1. - 2020. - С.111-114.

16. Чернова Е.В., Доколин А.С., Гаврилова И. В. Формирование в раннем подростковом возрасте готовности к обеспечению личной кибербезопасности // Информатика и образование, №7. -2018. - С.16-26.

17. Алекперов И.Д. Горбачева А.А. Типы угроз кибербезопасности и способы борьбы с хакерством// Прикладные аспекты мягкого моделирования в управлении в условиях цифровой трансформации, №2. -2021. - С.34-40.

18. Cybersecurity Challenge: Countering Digital Terrorism. United Nations. (2019),Vienna. URL:https://ideas.unite.un.org/counterdigiterrorism/Page/Home

References

1. Dubinina D. B. Problema mediabezopasnosti I kiberbezopasnosti lichnosti shkol'nika I studenta v sovremennom informatsionnom prostranstve [The problem of media security and cybersecurity of a student's and a student's personality in the modern information space] Ecologiya mediasredy: materialy IV otkrytoi mezhvuzovskoi nauchno-prakticheskoi konferentsii [Ecology of the media environment: materials of the IV Open Interuniversity Scientific and Practical conference], 96-101 (2019) [in Russian]

2. Moiseeva N. A. Kiberbezopasnost' kak vazhnyi component tsifrovoi gramotnosti pokoleniya Z, Tsifrovizatsiya I kiberbezopasnost': sovremennaya teoriya I praktika [Cybersecurity as an important component of digital literacy of generation Z, Digitalization and cybersecurity: modern theory and practice] Sbornik mezhdunarodnoi nauchno-prakticheskoi konferentsii [International Scientific and Practical Conference], 191-196, (2021) [in Russian]

3. [Electronic resource] Available at: https://1cert.ru/novosti/iso-27032-2012-privatnost-v-eru-vsepronikayushchey-informatsii?utm_referre (Accessed: 24.04.2023) [in Russian]

4. Seti kommunikatsionnye promyshlennye (Zshshishennost' (kiberbezopasnost') seti I sistemy) [Industrial communication networks (Security (cybersecurity) networks and systems)] (Standartinform, M., 2014, 80 p.) [in Russian]

5. Putyato M.M., Makaryan A.C. Kiberbezopasnost' kak neot'emlemyi atribut mnogourevnevogo zashishennogo kiberprostranstva [Cybersecurity as an Integral Attribute of Multilevel Protected Cyberspace] CASPIAN JOURNAL: Control and High Technologies, 3 (51), 94-102 (2020) [in Russian]

6. [Electronic resource] Available at: https://www.tadviser.ru/index.php/ [Электронный ресурс] (Accessed: 24.04.2023) [in Russian]

7. [Electronic resource] Available at: https://cyberleninka.ru/article/n/rukovodyaschie-ukazaniya-po-kiberbezopasnosti-v-kontekste-iso-27032/viewer (Accessed: 24.04.2023) [in Russian]

8. [Electronic resource] Available at: https://learn.microsoft.com/ru-ru/compliance/regulatory/offering-nist-csf (Accessed: 24.04.2023) [in Russian]

9. [Electronic resource] Available at: https://ru.wikipedia.org/wiki/ISO/IEC_27001 (Accessed: 24.04.2023) [in Russian]

10. [Electronic resource] Available at: https://en.wikipedia.org/wiki/IEC_62443 (Accessed: 24.04.2023) [in Russian]

11. Voskrekasenko O.A., Kireeva A.A., Shchelina T.T. Formirovanie kul'tury kiberbezopasnosti v sisteme profissional'noi podgotovki obuchayuschikhsya kolledzha kak pedagogicheskaya problema [Formation Of Cybersecurity Culture in The System of Vocational Training of College Students as a Pedagogical Problem] Sovremennye naukoemkie tekhnologii [Modern High-Tech Technologies], 10. 125-128, (2022) [in Russian]

12. Cybersecurity and New Technologies. Office of Counter-Terrorism. [Electronic resource] Available at: https://www.un.org/counterterrorism/ru/cct/programme-projects/cybersecurity (Accessed: 24.04.2023) [in Russian]

13. Gubenkov A. O., Lukyanova V.V. Aktual'nye problem kiberbezopasnosti v sotsial'nykh setyakh [Actual Problems Of Cybersecurity In Social Networks] Avtonomnaya lichnost' [Personality Autonomy], 3(26), 46-53, (2021) [in Russian]

14. Matkarimov A., Berdieva B., Ashyrova M. Basics of Cyber Security and Its Need // Cognitio Rerum, 3, 111-114, (2023) [in English]

15. Vorob'eva I.A., Sazonov A. Metody sotsial'noi inzhenerii v kontekste kiberbezopasnosti: informatika, vacheslitel'naya tekhnika I upravlenie [Methods of Social Engineering in the Context of Cybersecurity Informatics and Computer Engineering and Management] Estestvennye I tekhnicheskie nauki [Natural and Technical Sciences], 1, 111-114, (2020) [in Russian]

16. Chernova E.V., Dokolin A.S., Gavrilova I.V. Formirovanie v rannem podrostkovom vozraste gotovnosti k obespecheniyu lichnoi kiberbezopasnosti [Formation of Readiness to Ensure Personal Cybersecurity in Early Adolescence] Informatika I obrazovanie [Informatics and Education], 7, 16-26, (2018) [in Russian]

17. Alekperov I.D. Gorbacheva A.A. Tipy ugroz kiberbezopasnosti I sposoby bor'by s khakerstvom [Types of Cybersecurity Threats and Ways to Combat Hacking] Prikladnye aspekty myagkogo modelirovaniya v upravlenii v usloviyakh tsifrovoi transformatsii [Applied Aspects of Soft Modeling in Management in Conditions of Digital Transformation], 2, 34-40, (2021) [in Russian]

18. Cybersecurity Challenge: Countering Digital Terrorism. United Nations. (2019), Vienna. [Electronic resource] Available at: https://ideas.unite.un.org/counterdigiterrorism/Page/Home (Accessed: 24.04.2023) [in English]

Р.Е. Садықова

Eurasian Communications centre, Астана, Қазақстан

БҰҰ-ның терроризмге қарсы күрес жөніндегі жаһандық міндеттерін шешудегі киберқауіпсіздік мәселелері

Аңдатпа. Бүгінгі таңда киберқауіпсіздік қатерлері барлық елдердің алдында тұрған негізгі мәселелердің бірі болып табылады. Киберкеңістік біздің қазіргі өмірімізде маңызды рөл атқарады, бүкіл әлемдегі адамдар мен қауымдастықтарды біріктіріп, оларға әлеуметтену мен өзін-өзі ұйымдастыруға мүмкіндік береді.

Бұл мақалада кибершабуылдар мен қауіптердің негізгі түрлері, сондай-ақ олардың алдын алу әдістері ұсынылған. Киберқылмыстың әртүрлі түрлерімен, сондай-ақ кибертерроризммен күресу үшін қажетті әрекеттер қарастырылады.

Киберқылмыскерлер кибершабуылдарды жүзеге асыру үшін әртүрлі әдістер мен құралдарды белсенді қолданады, соның ішінде жүйелерге рұқсатсыз қол жеткізу, жеке ақпаратты ұрлау, қаржылық алаяқтық және зиянды бағдарламалық жасақтаманы тарату.

Кибертерроризм де қоғамға қауіп төндіреді, өйткені кибершабуылдар хаос тудыру және мемлекеттік институттар, денсаулық сақтау жүйелері, энергетика және т.б. сияқты маңызды инфрақұрылымдардың жұмысын бұзу үшін пайдаланылуы мүмкін.

Киберқауіпсіздікті қамтамасыз ету үшін мемлекеттік және халықаралық деңгейде ынтымақтастық қажет. Мемлекеттік деңгейдегі ынтымақтастық қауіп-қатер туралы ақпарат алмасудың бірлескен бастамаларын, киберқауіпсіздік мамандарының біліктілігін арттыру үшін бірлескен жаттығулар және киберқауіпсіздік бойынша жалпы стандарттар мен саясаттарды әзірлеуді қамтиды. Халықаралық деңгейде БҰҰ, Еуропалық Одақ, НАТО және басқалары сияқты әртүрлі елдер мен халықаралық ұйымдар арасында диалог орнату маңызды. Бұл стратегияларды үйлестіруге, кибершабуылдардың алдын алу және оларға ден қою жөніндегі шараларды үйлестіруге мүмкіндік береді.

Түйін сөздер: киберкеңістік, киберқауіпсіздік қатерлері, кибертерроризм, киберқауіпсіздік бойынша ынтымақтастық.

R.E. Sadykova
Eurasian Communications centre, Astana, Kazakhstan

Cybersecurity issues in addressing the global challenges of the un in the fight against terrorism

Abstract. Today, cybersecurity threats are one of the main problems faced by all countries. Cyberspace plays an important role in our modern life, uniting people and communities around the world, providing them with the opportunity for socialization and self-organization.

This article highlights the main types of cyberattacks and threats, as well as suggests methods to prevent them. Various types of cybercrimes are considered, as well as the necessary actions to combat cyberterrorism.

Cybercriminals actively use various methods and techniques to carry out cyber attacks, including unauthorized access to systems, theft of personal information, financial fraud and the distribution of malicious software.

Cyberterrorism is also a danger, since cyber attacks can be used to create chaos and disrupt the functioning of critical infrastructures, such as government institutions, healthcare systems, energy, and so on.

To ensure cybersecurity, cooperation is necessary both at the state and at the international level.

Cooperation at the state level includes joint initiatives to exchange information about threats, joint trainings and exercises to improve the skills of cybersecurity specialists, as well as the development of common standards and policies in the field of cybersecurity.

At the international level, it is important to establish a dialogue between various countries and international organizations, such as the UN, the European Union, NATO and others. This will allow us to coordinate strategies, coordinate measures to prevent and respond to cyber attacks.

Keywords: cyberspace, cybersecurity threats, cyberterrorism, cybersecurity cooperation.

Сведения об авторе:

Садыкова Р.Е. **–** PhD, советник, Eurasian Communications centre, Астана, Казахстан.

Sadykova R.E. **–** PhD, Advisor, Eurasian Communications centre, Astana, Kazakhstan.