ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

жаңартып отыру оның соңғы қауіпсіздік стандарттарына сәйкес келуіне және пайдаланушыларды жаңа қауіптерден қорғауға көмектеседі.

Қорытынды. Мақалада айтылып кеткен деректерге сүйенетін болсақ, қауіпсіздік назар аударуды қажет ететін жалғыз аспект емес. Құпия сөз менеджерін әзірлеуде пайдаланушы тәжірибесі де маңызды рөл атқарады. Әзірлеушілер пайдаланушыларға тіркелгі деректерін оңай басқаруға және қажетті ақпаратқа қол жеткізуге мүмкіндік беретін интуитивті және қолдануға оңай интерфейс жасауға ұмтылуы керек.

Сонымен қатар, пайдаланушыларды ақпараттық қауіпсіздік негіздерімен таныстыру жалпы қауіпсіздікті жақсартуда маңызды рөл атқарады. Пайдаланушылар құпия сөзді қорғау тәсілдері, әлсіз құпия сөздерді пайдалану қаупі және олардың тіркелгілеріне шабуылдардың алдын алу әдістері туралы білім алуы керек. Тұрақты ақпараттық науқандар мен оқу материалдары пайдаланушылардың хабардарлығын арттыруға және онлайн ортаны барлығы үшін қауіпсіз етуге көмектеседі.

Сонымен, мақаланың қорытындысында қауіпсіз құпия сөз менеджерлерін әзірлеудің техникалық аспектілері ғана емес, сонымен қатар мобильді қосымшаларда тіркелгі деректерін тиімді және қауіпсіз пайдалануды қамтамасыз ететін пайдаланушылардың рөлін түсіну және оларды оқыту маңыздылығына баса назар аударылады.

Пайдаланылған әдебиеттер тізімі

1. Ayyagari R. Why Do Not We Use Password Managers? A Study on the Intention to Use Password Managers / R. Ayyagari // Contemporary Management Research. 2019. P. 227–245.
2. Bahmanziari T.P. Is Trust Important in Technology Adoption? A Policy Capturing Approach / T.P. Bahmanziari // Journal of Computer Information Systems. 2003. № 43(4). P. 46–54
3. "Безопасность мобильных приложений" Гупта, Химаншу (2019). P. 127–144
4. "Руководство хакера веб-приложений: Поиск и использование уязвимостей" Статтард, Дафидд и Пинто, Маркус (2014).
5. Разработка менеджера паролей под Android. https://habr.com/ru/articles/328708/

УДК 004.056

ИССЛЕДОВАНИЕ КИБЕРУГРОЗ ДЛЯ ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ ДЕЯТЕЛЬНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ИНФРАСТРУКТУР

Тұрарғазинов Жандос Серікқазыұлы
turargazinov_zhs@enu.kz
Магистрант Евразийского национального университета им. Л. Н. Гумилева,
Астана, Казахстан
Научный руководитель-к.ф-м.н., ассоциированный профессор, Сатыбалдина Д.Ж.

Аннотация

В данной статье осуществляется комплексный анализ киберугроз, с которыми сталкиваются критически важные инфраструктуры Республики Казахстан. Особое внимание уделяется идентификации основных типов кибератак, в частности, доминирующему влиянию фишинговых операций, и их воздействию на непрерывность функционирования жизненно важных секторов экономики и социальной сферы. В работе представлен обзор текущего состояния кибербезопасности в стране, включая анализ недавних инцидентов и мер реагирования на них. Основываясь на международном опыте и текущих тенденциях, предложены конкретные стратегии и решения для укрепления киберустойчивости критически важных инфраструктур Казахстана. Рекомендации включают разработку и внедрение национальных стандартов кибербезопасности, обучение и повышение осведомленности сотрудников, усиление межведомственного и международного сотрудничества, применение современных технологий защиты и разработку планов реагирования на инциденты. Статья подчеркивает необходимость комплексного подхода к обеспечению кибербезопасности,

сочетающего в себе национальные и международные усилия для эффективной защиты от киберугроз в современном цифровом мире.

Ключевые слова: киберугрозы, кибербезопасность, критически важные инфраструктуры, Казахстан, фишинг, национальные стандарты, межведомственное сотрудничество, международное сотрудничество.

В современном мире, где технологии проникают во все сферы жизни, критически важная инфраструктура становится основой для поддержания социальной стабильности, экономического развития и национальной безопасности. В Казахстане, как и во многих других странах, к критически важной инфраструктуре относятся объекты энергетики, транспорта, информационных технологий, связи, финансовых услуг, а также системы здравоохранения и обеспечения жизнедеятельности населения. Эти сектора играют ключевую роль в поддержании функционирования государства и обеспечении благополучия его граждан.

С развитием цифровых технологий растет и уровень угроз, которым подвержены эти жизненно важные системы. Киберугрозы — это один из основных факторов риска для непрерывности деятельности критически важных инфраструктур. Они могут принимать различные формы, от вирусных атак и фишинга до сложных целенаправленных кибератак, целью которых является дестабилизация работы инфраструктур, кража конфиденциальных данных или даже физическое уничтожение объектов через удаленное управление их работой.

В контексте Казахстана, страны, активно развивающей свою цифровую инфраструктуру и внедряющей технологические инновации в экономику и управление государственными процессами, вопрос защиты критически важных инфраструктур от киберугроз приобретает особую актуальность. Последствия кибератак могут быть катастрофическими, вплоть до остановки жизненно важных служб, серьезных экономических потерь и, в крайних случаях, угрозы жизни и здоровью граждан.

В данной статье мы рассмотрим основные категории киберугроз, с которыми сталкивается Казахстан, и их потенциальное влияние на непрерывность работы критически важных секторов экономики и социальной сферы. Также будут исследованы текущие меры по обеспечению кибербезопасности и предложены рекомендации по дальнейшему укреплению защиты национальной инфраструктуры от киберугроз.

Международный опыт показывает, что защита критически важных инфраструктур от киберугроз является многоаспектной задачей, требующей комплексного подхода. В странах с развитой цифровой экономикой, таких как США, страны Европейского Союза, Япония и Южная Корея, разработаны и реализуются национальные стратегии кибербезопасности, включающие меры по защите критической инфраструктуры. Основными элементами таких стратегий являются развитие нормативно-правовой базы, укрепление межсекторального и международного сотрудничества, формирование системы раннего обнаружения и реагирования на киберугрозы, а также повышение уровня кибергигиены среди персонала и населения в целом[1].

Исследования, проведенные в рамках Европейского союза, показывают, что ключевым фактором успешной защиты критической инфраструктуры является сотрудничество между государственным и частным секторами, а также координация усилий на международном уровне[2]. Внедрение единых стандартов и практик, обмен информацией о киберугрозах и опыте противодействия им позволяет существенно повысить эффективность защитных мер.

Анализ существующих исследований по оценке и управлению киберрисками для инфраструктур критического назначения.

В области оценки и управления киберрисками для критически важных инфраструктур существует обширная научная литература, фокусирующаяся на методологиях количественной и качественной оценки угроз, уязвимостей и последствий кибератак. Одной из ключевых задач является разработка моделей и инструментов, позволяющих прогнозировать вероятность возникновения киберинцидентов и оценивать потенциальный ущерб от них[3].

Ряд исследователей подчеркивает важность учета специфики отдельных секторов критической инфраструктуры при разработке мер по управлению киберрисками. Так,

например, для сектора энергетики характерны угрозы, связанные с контролем за распределением и подачей энергии, в то время как для финансового сектора особую опасность представляют атаки на системы электронных платежей и кража конфиденциальной информации[4].

Важной тенденцией в области управления киберрисками является использование технологий искусственного интеллекта и машинного обучения для анализа больших данных о киберугрозах, что позволяет более эффективно предсказывать и предотвращать кибератаки[5].

Казахстан, активно развивающийся в цифровом направлении и внедряющий технологические инновации в экономику и управление государственными процессами, сталкивается с возрастающим количеством киберугроз, нацеленных на критически важные инфраструктуры. По данным кибердайджеста АО «Государственной технической службы» Комитета национальной безопасности Республики Казахстан, фишинг является одной из наиболее распространенных форм кибератак. Злоумышленники эксплуатируют недостаточную подготовленность сотрудников, используя фишинговые атаки для запуска вредоносного программного обеспечения, кражи учетных данных и получения доступа к корпоративным сетям или базам данных с конфиденциальной или персональной информацией.

Отмечается тенденция к распространению геотаргетированных фишинговых угроз, когда киберпреступники фокусируются на определенной локации, стремясь создать наиболее эффективную атаку. Эти атаки часто имитируют известные бренды или организации, используя доменные имена в национальной зоне .kz или .қаз, что делает их кажущимися легитимными и повышает вероятность успеха атаки. В ответ на угрозу фишинга и других кибератак государственные органы Казахстана и частные компании активизировали усилия по повышению уровня кибербезопасности. Основное внимание уделяется обучению сотрудников, улучшению технических средств защиты и внедрению комплексных систем обнаружения и предотвращения киберугроз. Разработаны и реализованы программы по повышению осведомленности о киберугрозах, а также созданы специализированные подразделения по реагированию на киберинциденты[6].

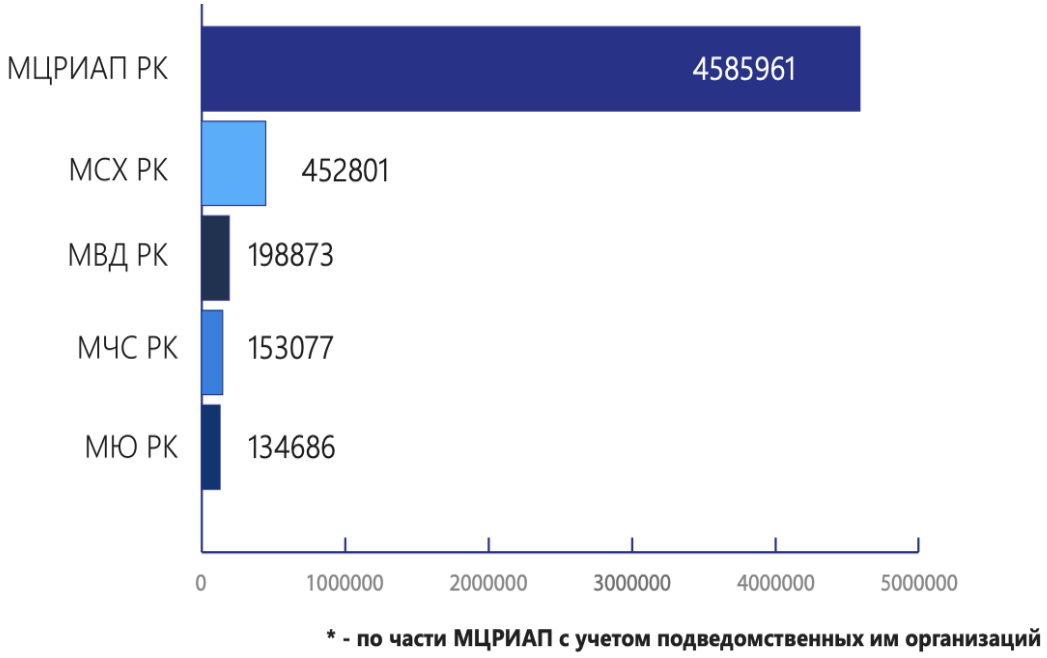

Рисунок 1. Топ-5 ГО по количеству событий связанных с ботнетами

В мире, где цифровые технологии проникают во все сферы жизни, кибербезопасность становится одной из ключевых проблем для государств, критических важных инфраструктур, организаций и частных лиц. В исследовании Positive technologies приведена актуальные киберугроз для стран Азия за 2022-2023 год. В последние годы страны Азии стали глобальными лидерами в области внедрения технологических инноваций, опережая весь остальной мир, но с развитием цифровых технологий в странах этого региона возрастает и необходимость в разработке и реализации устойчивых стратегий кибербезопасности.

Относительно малое количество атак (3%) приводило к прямым финансовым потерям — вследствие уплаты выкупа вымогателям или непосредственной кражи денег со счетов компании. Однако общий ущерб от кибератаки складывается из дополнительных расходов, включая затраты на реагирование, расследование, восстановление инфраструктуры, и убытков, связанных с вынужденным простоем и оттоком клиентов. Например, по оценкам IBM средняя стоимость одной утечки для компании в 2023 году в странах ASEAN составляет 3,05 млн долларов, а в Индии — 2,18 млн[7].

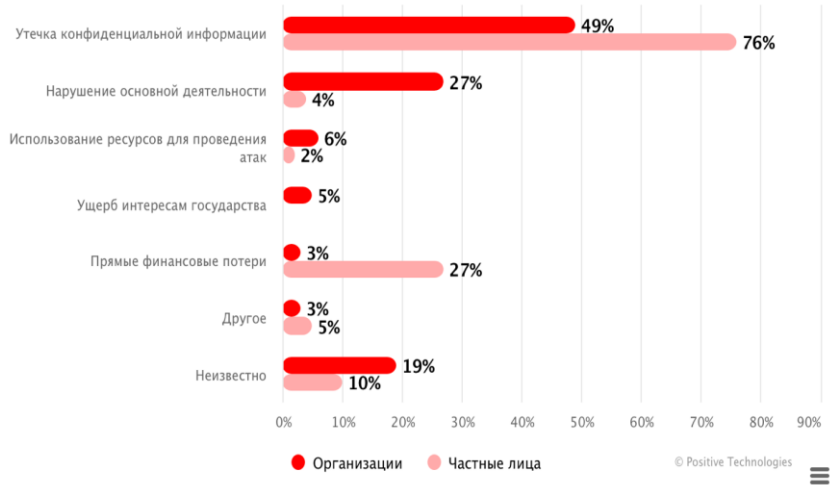

Рисунок 2. Последствия атак

С утечкой конфиденциальной информации сталкивались и обычные пользователи, причем к таким последствиям приводили 76% успешных атак. В 27% случаев пользователи теряли деньги в результате действий злоумышленников.

В рассматриваемый период с начала 2022 года по первое полугодие 2023-го жертвами атак среди организаций чаще всего становились госучреждения (22% от числа всех атак), промышленные компании (9%), IT-компании (8%) и финансовые организации (7%).

74% атак носили целенаправленный характер, то есть были нацелены на конкретные организации, отрасли или людей[7].

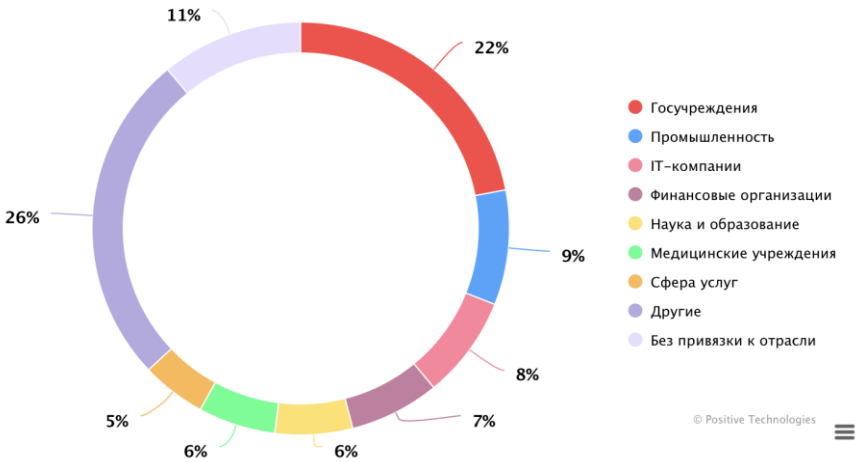

Рисунок 3. Категории жертв среди организаций

Для укрепления киберустойчивости критически важных инфраструктур в Казахстане, страна активно разрабатывает и внедряет национальные стандарты кибербезопасности, нацеленные на повышение уровня защиты от киберугроз. Важным аспектом является обучение и повышение осведомленности сотрудников о методах противодействия кибератакам, что включает в себя разработку программ обучения и кампаний по повышению кибергигиены. Кроме того, Казахстан активизирует усилия в области межведомственного и международного сотрудничества для обмена информацией о киберугрозах и совместной разработки мер по их нейтрализации, что позволяет стране интегрировать мировой опыт и лучшие практики в национальную систему кибербезопасности.

Использование современных технологий защиты, включая системы обнаружения вторжений и многофакторную аутентификацию, играет ключевую роль в защите критической инфраструктуры. Разработка и тестирование планов реагирования на инциденты кибербезопасности также являются важной составляющей общей стратегии защиты, позволяя организациям эффективно реагировать на кибератаки и минимизировать их последствия.

На международном уровне Казахстан принимает активное участие в различных инициативах и сотрудничает с международными организациями, такими как ОБСЕ, Интерпол и Глобальный альянс по кибербезопасности. Это сотрудничество позволяет стране обмениваться опытом, знаниями и информацией о киберугрозах, повышая тем самым эффективность национальных мер по обеспечению кибербезопасности.

Таким образом, Казахстан реализует комплексный подход к защите критически важных инфраструктур от киберугроз, включая разработку и внедрение стандартов и нормативных актов, повышение осведомленности и компетенций сотрудников, укрепление международного сотрудничества, а также применение современных технологий и методик защиты. Эти меры направлены на создание устойчивой и эффективной системы кибербезопасности, способной противостоять современным и будущим киберугрозам.

Список использованной литературы

1. Льюис Дж.А., Нойнек Г. "Кибербезопасность и защита критически важной инфраструктуры: сравнительный анализ международных подходов" // Журнал по безопасности родины и управлению чрезвычайными ситуациями, 2015.

2. Агентство Европейского Союза по кибербезопасности (ENISA) "Обзор угроз для критической инфраструктуры" // Агентство Европейского Союза по кибербезопасности (ENISA), 2020.

3. Кшетри Н. "Киберпреступность и кибербезопасность в глобальном Юге" // Palgrave Macmillan, 2013.

4. Ассанте М.Дж., Тоби Д.Х. "Усиление кибербезопасности критически важной инфраструктуры" // IEEE Безопасность и конфиденциальность, 2011.

5. Ван В. и др. "Искусственный интеллект для кибербезопасности: обзор" // Журнал науки и технологий в области компьютеров, 2019.

6. Государственная техническая служба Республики Казахстан "Кибердайджест за год" [Электронный ресурс] // Государственная техническая служба Республики Казахстан, 2022. https://sts.kz/wp-content/uploads/2023/01/year-2022-digest.pdf

7. Позитив Технологии "Кибербезопасность в Азии: аналитический обзор" [Электронный ресурс] // Позитив Технологии, 2023. https://www.ptsecurity.com/ru-ru/research/analytics/asia-cybersecurity-threatscape-2022-2023

УДК 004.056.5

БІЛІМ БЕРУ ПОРТАЛДАРЫНА SQL-ШАБУЫЛДАРЫН ЗЕРТТЕУ ӘДІСТЕМЕСІ

Тұрсынова Әселя Ғалымжанқызы
tursynova-2021@mail.ru