5 СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

УДК 004.056.5

Т. О. Авраменко
avramenko@gsu.by
Гомельский государственный университет имени Ф. Скорины, Республика Беларусь

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ В СТРАНАХ СНГ

В материале приведена аналитика реальных угроз информационной безопасности и инцидентов, с которыми сталкиваются организации стран-участниц СНГ в последние два года, а также раскрываются аналитические данные о количестве и видах кибератак.

В условиях стремительного технологического прогресса информационная безопасность становится одной из ключевых задач для организаций любого масштаба. Увеличение числа кибератак и утечек данных требует внимания к актуальным угрозам, их анализа и разработке эффективных стратегий защиты.

Информационная безопасность в организациях включает в себя комплекс мероприятий и стратегий, предназначенных для защиты конфиденциальной информации, а также гарантии её доступности, целостности и подлинности. Это многогранное понятие охватывает различные аспекты, такие как предотвращение несанкционированного доступа, кибератак и утечек данных.

Угрозой информационной безопасности называют потенциальное действие или событие, которое может привести к ущербу для информационных систем, данных или инфраструктуры организации. Оно может включать в себя как намеренные атаки злоумышленников, так и случайные инциденты, происходящие в результате небрежности или технических сбоев.

Рассмотрим конкретные данные, отражающие реальные угрозы и инциденты, с которыми сталкиваются организации в старнах СНГ в 2023 г. – первом полугодии 2024 г. На сегодняшний день интерес преступников к странам СНГ неуклонно растёт из квартала в квартал. В II квартале 2024 года количество атак увеличилось в 2,6 раза по сравнению с аналогичным периодом 2023 года (рисунок 1) [1].

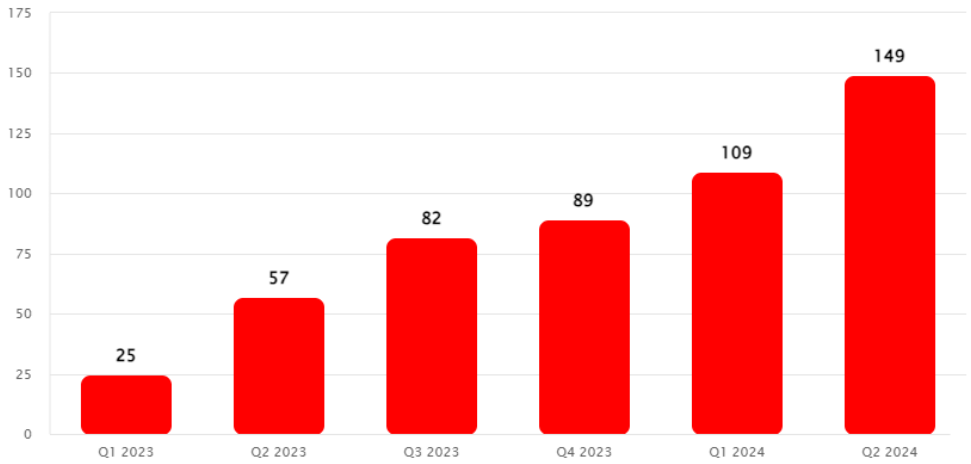

Рисунок 1 – Распределение количества успешных кибератак по кварталам в 2023–2024 гг. на территории стран СНГ

Согласно данным компании Positive Technologies, одного из ведущий разработчиков продуктов, решений и сервисов в сфере кибербезопасности в Российской Федерации, 73 % всех атак на организации СНГ были направлены на Россию, в то время как Казахстан и Беларусь заняли второе и третье места с долями 8 % и 7 % соответственно (рисунок 2). Увеличение интереса к этим странам также подтверждается значительным количеством объявлений в даркнете о реализации и приобретении персональных данных и услуг, связанных с Россией, Беларусью и Казахстаном [1].

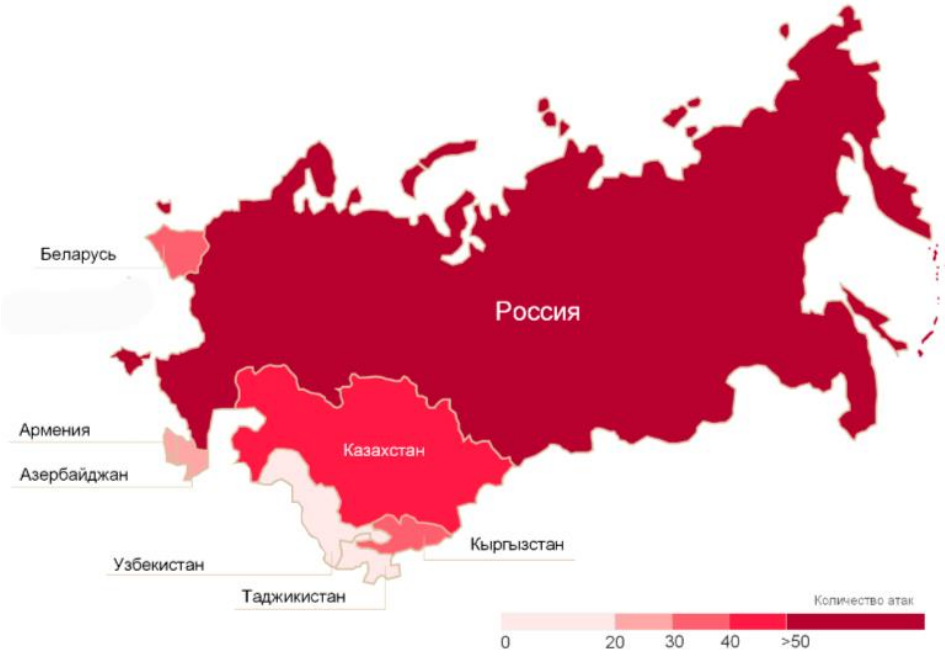

Рисунок 2 – Распределение успешных кибератак по странам СНГ в 2023–2024 гг.

В целом, в 2023 г. и первой половине 2024 г. от наибольшего количества кибератак в странах СНГ пострадали госучреждения (18 %), промышленность (11 %) и телекоммуникационные компании (10 %). Из-за того, что эти организации имеют ключевое значение для экономики стран, а также из-за хранения в них большого количества конфиденциальных данных, эти отрасли представляют наибольший интерес для киберпреступников.

В 41 % случаев успешные атаки на организации заканчивались утечкой конфиденциальной информации, в 37 % случаев – нарушением деятельности организаций. При этом, более половины объёма похищенных данных составили персональные данные (30 % от общего объёма похищенной информации) и коммерческая тайна (29 % от общего объёма похищенной информации). В то же время результатом атак на физических лиц становились утечки персональных данных в 69 % случаев и финансовые потери в 32 % случаев.

Около 18 % кибератак на организации в странах СНГ пришлось на государственный сектор, при этом почти две трети из них (62 %) совершены с применением вредоносного программного обеспечения, а в 57 % успешных атак использовались методы социальной инженерии. Кроме того, каждая пятая атака на учреждения госсектора – это DDoS. Ущерб интересам государства причинили 28 % атак, а 22 % стали результатом нарушения деятельности госучреждений [1].

Промышленный сектор экономики, также как и государственный, уже традиционно находится в зоне повышенного внимания киберпреступников, и страны СНГ не исключение. Около 11 % кибератак на организации в странах СНГ пришлось именно на промышленность. При этом в 79 % атак применялось вредоносное программное обеспечение, из них в 42 % применялись инфостилеры, на долю использования вредоностного программного обеспечения для удалённого доступа пришлось 37 %, а шифровальное программное обеспечение использовалось в 26 % случаев [2].

Телекоммуникационные компании становились жертвами в среднем каждой десятой атаки на организации стран СНГ. Основным видом атак, используемых против организаций отрасли, стали DDoS-атаки и составили 43 % от всех атак на отрасль. При этом утечка конфиденциальных данных происходила, в среднем, в каждом четвёртом случае.

Таким образом, среди основных видов кибератак в странах СНГ можно выделить применение вредоносного программного обеспечения и методов социальной инженерии. Однако присутствует особенность, присущая региону: количество DDoS-атак здесь выше, чем в мире и составляет порядка 18 % от общего объёма атак (против общемировых 8 %). Такое увеличение показателя может быть связано с текущей геополитической обстановкой в регионе (рисунок 3).

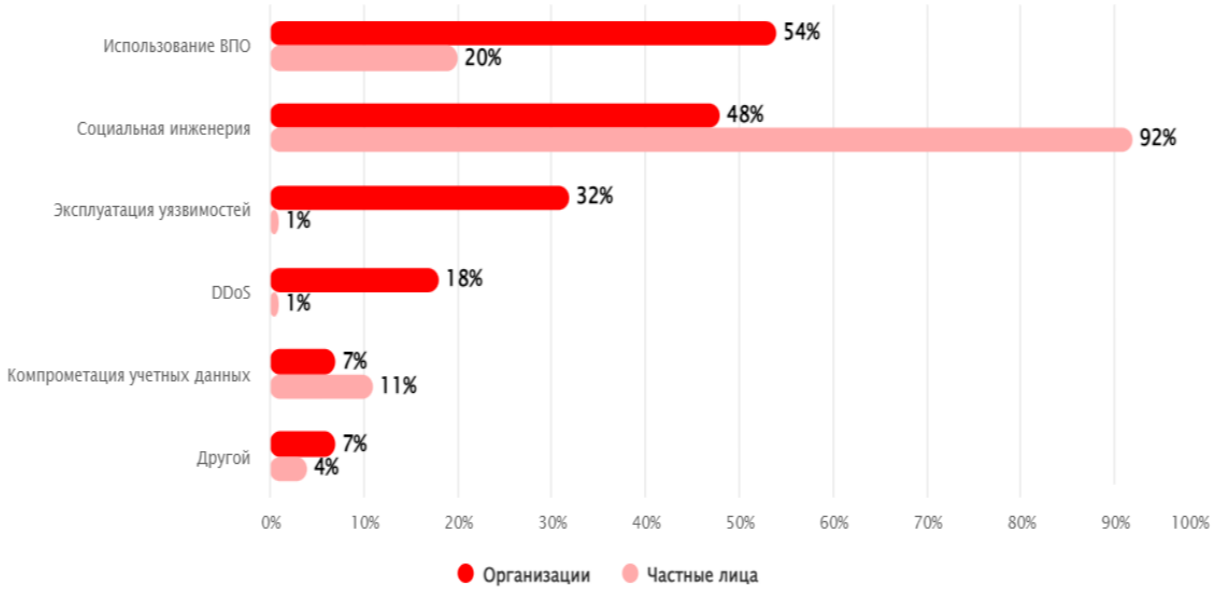

Рисунок 3 – Методы кибератак на страны СНГ

На сегодняшний день, Беларусь занимает 70-е место в рейтинге Национальных индексов кибербезопасности (NSCI), уступая только Азербайджану и России среди стран СНГ [3]. В феврале 2023 года в Беларуси совместно с Российской Федерацией было утверждено постановление о сотрудничестве в сфере информационной безопасности, среди основных целей которого усиление защиты от внешних угроз, укрепление и обеспечение системы информационной безопасности Союзного государства. Также в феврале 2023 года в Беларуси был подписан Указ № 40 «О кибербезопасности», который определяет создание национальной системы обеспечения информационной безопасности страны. При этом, уже более 14 лет в стране функционирует Национальный центр обмена трафиком (НЦОТ), главная задача которого состоит в развитии единой республиканской сети передачи данных.

За 2023 г. – первое полугодие 2024 г. в Беларуси каждой пятой атаке подвергались государственные учреждения (22 %), немного меньше случаев кибератак зарегистрировано в промышленном секторе (14 %). При этом, в 76 % от всех кибератак в стране применялось вредоносное программное обеспечение, а в результате почти каждой второй атаки (57 %) происходила утечка конфиденциальной информации (рисунок 4) [1].

Самую значительную угрозу для организаций в стране представляют кибершпионские группы XDSpy, Lazy Koala, Sticky Werewolf и другие. Так, например, в начале 2024 года компания Avast, разработчик программы CCleaner, приостановила деятельность на территории России и Беларуси. Инфоповод был использован киберпреступниками из группы Sticky Werewolf. Группировкой была организована фишинговая кампания, от которой пострадали белорусские организации. В ходе этой кампании под видом программы CCleaner распространялся троян Ozone RAT.

Рисунок 4 – Сводная статистика по кибератакам на Республику Беларусь в 2023–2024 гг.

Однако кибершпионаж не единственная значительная угроза для организаций в Беларуси. Информационной безопасности страны угрожают также атаки группировок так называемых хактивистов. Так, в конце 2023 года в результате одной из атак был взломан сайт госагенства БелТа и похищены 90 Гбайт конфиденциальной информации, в том числе персональные данные сотрудников. Чуть позже, в апреле 2024 года хактивисты заявляли об атаке на крупнейшее в стране предприятие по производству удобрений «ГродноАзот».

В заключении стоит отметить, что, несмотря на происходящие в последние годы в странах СНГ геополитические преобразования, стремительное цифровое развитие региона в целом и Беларуси в частности всё больше привлекает внимание киберпреступников. С каждым кварталом количество атак на организации стран СНГ растёт, в связи с чем перед государствами и организациями стоит важная и актуальная задача обеспечения и усиления защиты информационной безопасности.

Литература

1. Positive Technologies [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/#id10. – Дата доступа: 29.09.2024.

2. Sophos News [Электронный ресурс]. - Режим доступа: https://news.sophos.com/en-us/2024/05/28/the-state-of-ransomware-in-manufacturing-and-production-2024/. – Дата доступа: 29.09.2024.

3. National Cyber Security Index [Электронный ресурс]. – Режим доступа: https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1. – Дата доступа: 29.09.2024.

УДК 339.138

В. М. Войтович
vadim.vm1@mail.ru
ИПКиПКЗ Белорусского государственного медицинского университета, Республика Беларусь

ЦИФРОВИЗАЦИЯ МАРКЕТИНГА: НОВАЯ ЭРА ВЗАИМОДЕЙСТВИЯ С ПОТРЕБИТЕЛЯМИ

Статья посвящена процессам цифровизации маркетинга. В ней рассматриваются ключевые аспекты цифровой трансформации, включая использование аналитики больших данных, искусственного интеллекта, автоматизации процессов, а также внедрение цифровых каналов взаимодействия с клиентами.