29. КИБЕРПРЕСТУПНОСТЬ КАК ГЛОБАЛЬНАЯ УГРОЗА

Марушина А. Д.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Жилинская Н. Н. – канд. экон. наук

Аннотация. По мере того, как общество продолжает мигрировать в цифровой мир, угроза киберпреступности становится все более ощутимой, и обычно стоит организациям десятки, а то и сотни миллионов долларов. Согласно ведущему исследовательскому центру мировой киберэкономики Cybersecurity Ventures, глобальные затраты на киберпреступность будут расти на 15 процентов в год, достигнув 10,5 трлн долларов США в год к 2025 году по сравнению с 3 трлн долларов США в 2015 году [1]. Однако наблюдаются не только экономические потери, в опасности находятся ключевая инфраструктура общества, доверие общественности к цифровой трансформации и общее доверие к технологиям. А низкие входные барьеры для субъектов киберугроз, более враждебные методы атак, нехватка профессионалов в области кибербезопасности — все это усугубляет риск.

Человечество все больше полагается на технологии для управления всеми аспектами жизни – от коммунальных услуг до бизнес-процессов и даже покупок продуктов. Применение цифровых

технологий для реализации товаров и услуг, оказания государственных услуг, образования граждан позволяет всему обществу приобрести так называемые цифровые дивиденды. Однако любые информационные и технические новшества значительно расширяют сферу киберпреступности и создают условия для повышения эффективности её осуществления. Повсеместное использование облачных технологий и хранилищ данных привело к распространению киберпреступности не только среди финансовых организаций, но и среди предприятий обрабатывающей, сельскохозяйственной и прочих промышленностей.

По данным Всемирного обзора экономических преступлений PricewaterhouseCoopers (PWC) за 2022 г., для организаций любого размера наибольшую угрозу представляет киберпреступность, за которой следуют мошенничество с клиентами и незаконное присвоение активов [2]. При этом наибольшую долю среди экономических преступлений киберпреступность занимает в секторе ИКТ и телекоммуникационной отрасли (50 %) и отрасли здравоохранения (40 %), что обусловлено ценностью медицинских данных, легкостью взлома техники и неосведомленностью сотрудников об кибербезопасности.

Киберпреступность по определению игнорирует национальные границы, а значит, связанные с ней кризисы непременно будут иметь глобальный характер. В настоящее время технологии используются совместно множеством организаций. Следовательно, у этих организаций возникают общие зависимости. Например, в июле 2021 года супермаркеты в Швеции были вынуждены закрыть свои двери после кибератаки на поставщика ИТ-услуг Kaseya, базирующегося во Флориде, США. Данное событие демонстрирует результат зависимости предприятий от услуг другой организации.

Глобальные ежегодные издержки киберпреступности оцениваются в 6 триллионов долларов в год [3]. Однако существует несколько трудностей при составлении точной оценки затрат на киберпреступность. Во-первых, многие организации отказываются сообщать о том, что они стали жертвами киберпреступности, дабы не наносить ущерб своей репутации. По-прежнему трудно получить точные данные на национальном уровне. Другая проблема заключается в том, что трудно оценить фактическую стоимость того, что люди избегают онлайн-транзакций из-за страха стать жертвой киберпреступности.

Компания IBM Security изучила 550 организаций, пострадавших от утечек данных, произошедших в период с марта 2021 по март 2022 года. Утечки данных произошли в 17 странах и регионах и в 17 различных отраслях промышленности [4]. Примечательно, что впервые исследование показывает следующие выводы: 83% исследованных организаций имели более одной утечки данных; 60% нарушений, допущенных организациями, привели к повышению цен, что легло на плечи клиентов.

Самая высокая средняя стоимость утечки данных наблюдается в отрасли здравоохранения. С 2021 по 2022 г. она выросла на 9,4%. Финансовые организации являются вторыми по величине расходов, за ними следуют фармацевтическая, технологическая и энергетическая отрасли.

Понимание различных типов киберпреступлений – является первым шагом для обеспечения безопасности своей компании. На данный момент наиболее распространены следующие виды киберпреступлений:

– Фишинг – вид интернет-мошенничества, цель которого — получить идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации.

– Программа-вымогатель – это разновидность вредоносного ПО, которое атакует компьютерные системы, блокирует данные и требует оплаты за их разблокировку.

– Хакинг – это акт получения несанкционированного доступа к компьютерной системе с целью заражения ПК жертвы или обхода мер безопасности.

– Криптоджекинг – это тип киберпреступления, при котором хакеры незаконно используют компьютеры и сети людей для получения криптовалюты.

– Взлом IoT-устройств – ситуация, когда хакер использует устройство, подключенное к Интернету, такое как умный термостат или холодильник. Он взламывает устройство и заражает его вредоносным ПО, который распространяется по всей сети.

– DDoS – кибератака, которая нарушает доступность онлайн-сервисов или систем, перегружая сервер огромным объемом трафика. Чтобы запустить DDoS-атаку, злоумышленники должны сначала взять под контроль несколько компьютерных систем, включая устройства Интернета вещей.

Самой распространенной атакой, связанной с утечками данных, в 2022 году была кража учетных данных [5]. Деструктивные вредоносные ПО ответственны за 17% от общих атак, направленных на организации. Еще 19% утечек были вызваны атаками на цепочки поставок. Человеческие ошибки, то есть нарушения, вызванные непреднамеренно из-за небрежных действий сотрудников организации, несут ответственность за 21% утечек.

Многие организации недостаточно хорошо подготовлены к киберкризисам. Для руководителей по всему миру риски, связанные с безопасностью данных, возрастают быстрее, чем они способны их снизить. Основные причины этому:

рост партнеров и поставщиков (руководители бизнеса признают, что на риск кибербезопасности их организации влияет качество безопасности во всей цепочке поставок их коммерческих партнеров и клиентов);

отсутствие поддержки руководством проблемы кибербезопасности;

конвергенция цифровых и физических систем, обеспечиваемая технологией Интернета вещей, повышающая подверженность их организации киберрискам;

нехватка квалифицированных работников.

Проблемы обеспечения кибербезопасности варьируются в зависимости от сферы деятельности предприятия. Каждая отрасль имеет свой собственный уникальный набор задач в области кибербезопасности. Самые большие проблемы кибербезопасности, с которыми сейчас сталкиваются организации в зависимости от отрасли: отсутствие приоритезации киберрисков – технологическая отрасль; незащищённый доступ к базам данных, внутренние утечки информации, в силу недостаточной культуры кибербезопасности у медперсонала – здравоохранение; растущая уязвимость цепочек поставок – розничная торговля; нехватка квалифицированных специалистов по кибербезопасности – сфера финансов, страхования.

Стоимость последствий взлома по своей сути являются более разрушительным с финансовой точки зрения, чем оплата кибербезопасности, которая предотвращает нарушения. Стоимость кибербезопасности учитывается в ИТ-бюджете организации, а стоимость восстановления после нарушения безопасности — нет. Поэтому организациям выгоднее предотвратить кибератаку, нежели ликвидировать её последствия.

Меры защиты, которые организации могут предпринять, чтобы помочь снизить финансовые затраты и репутационные последствия утечки данных:

– Киберстрахование. Если небольшая организация столкнется с кибератакой с последующими последствиями для более крупных организаций, она получит помощь в восстановлении в виде страховой выплаты. На данный момент компания Chubb, базирующаяся в Цюрихе, является одним из крупнейших поставщиков киберстрахования с долей рынка в примерно 12% [6].

– Внедрение модели безопасности с нулевым доверием, чтобы помочь предотвратить несанкционированный доступ к конфиденциальным данным. Доктрина «тотального недоверия» предписывает видеть потенциальную угрозу в любой попытке получить доступ к корпоративной информации до тех пор, пока не будет доказано обратное.

– Инвестирование в Искусственный интеллект и автоматизацию. Применение ИИ ускорит поиск угроз и тестирование на проникновение, а также фильтрацию ложных срабатываний инструментов безопасности. По данным IBM, организации с полностью развернутым искусственным интеллектом безопасности и автоматизацией имели среднюю общую стоимость утечки данных в размере 3,15 миллиона долларов США, по сравнению с 6,20 миллионами долларов США для организаций, в которых они не применяются [4].

– Создание в организациях группы реагирования на инциденты (IR teams) и тестирование разрабатываемого ею плана реагирования для повышения киберустойчивости. Разработав подробный план действий в случае кибератак, организации могут быстрее решать возникающие проблемы.

В заключении стоит отметить, что комплексная программа борьбы с киберпреступностью должна включать совокупность действий, как частного сектора экономики, так и государственных структур. Разработка нормативно-правовой базы, включающей законодательство, определяющее, что представляют собой незаконная деятельность в киберпространстве, инструменты для расследования, судебного преследования и обеспечения соблюдения такого законодательства, и установление базовых показателей кибербезопасности будут содействовать защите общества и благоприятствовать созданию безопасной цифровой среды. В свою очередь предприятиям частного сектора для демонстрации своей устойчивости, означающей способность дать отпор кибератаке и быстро восстановиться, используя имеющиеся ресурсы, придется постоянно инвестировать в свои стратегии кибербезопасности и, возможно, полностью перестроить свои бизнес-процессы.

Список использованных источников:

1.Cybercrime To Cost The World $10.5 Trillion Annually By 2025 [Electronic resource]. – Mode of access: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/. - Date of access: 18.02.2023.

2.Global Cybersecurity Outlook 2022 [Electronic resource]. – Mode of access: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf. – Date of access: 19.02.2023.

3.Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021 [Electronic resource]. - Mode of access: https://cybersecurityventures.com/annual-cybercrime-report-2020. – Date of access: 19.02.2023.

4.Cost of a Data Breach Report 2022 [Electronic resource]. - Mode of access: https://www.ibm.com/downloads/cas/3R8N1DZJ. - Date of access: 14.03.2023.

5.The biggest cyberattacks of 2022 [Electronic resource]. - Mode of access: https://www.bcs.org/articles-opinion-and-research/the-biggest-cyber-attacks-of-2022/. – Date of access: 17.02.2023.

6.Ведущие компании, предлагающие киберстрахование [Электронный ресурс]. – Режим доступа: https://ru1.templeprotestant.org/top-companies-offering-cyber-insurance-5453#menu-3. – Дата доступа: 15.03.2023.