КИБЕРПРЕСТУПНОСТЬ КАК ОСНОВНАЯ УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СОВРЕМЕННОГО ГОСУДАРСТВА

Г. Г. Головенчик

Белорусский государственный университет,
ул. Ленинградская 20, 220030, г. Минск, Беларусь, goloventchik@bsu.by

Рассматривается такая глобальная угроза обеспечению национальной безопасности государства, как киберпреступность, ввиду масштабов ее распространения, глубины и проблематичности противодействия. Проанализированы основные тренды в сфере киберпреступности в условиях информатизации всех сфер жизни современного общества. Акцентировано внимание на смене парадигмы кибербезопасности в условиях ускорения цифровой трансформации.

Ключевые слова: интернет; киберпреступность; кибербезопасность; кибератака.

CYBERCRIME AS THE MAIN THREAT TO THE NATIONAL SECURITY OF A MODERN STATE

G. G. Goloventchik

Belarusian state University,
20 Leningradskaya str., 220030, Minsk, Belarus, goloventchik@bsu.by

Such a global threat to the national security of the state as cybercrime is considered, due to the scale of its spread, the depth and problematic nature of counteraction. The main trends in the field of cybercrime in the conditions of informatization of all spheres of life of modern society are analyzed. Attention is focused on the paradigm shift of cybersecurity in the context of accelerating digital transformation.

Keywords: Internet; cybercrime; cybersecurity; cyberattack.

В последние годы всё большее подтверждение находит тезис о том, что технические инновации могут быть использованы как для социального блага, так и с противозаконными целями. Это более чем верно в отношении киберпреступности, которая становится всё более агрессивной и представляет всё большую угрозу национальной безопасности современного государства.

По определению лаборатории Касперского, «киберпреступление – это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства».

Многие исследователи справедливо утверждают, что COVID-19 ускорил Четвертую промышленную революцию, расширяя цифровизацию человеческого взаимодействия, электронной коммерции, онлайн-образования и удаленной работы. Подсчитано, что использование интернета во всем мире в 2020 г. увеличилось на 30%, в то время как объем электронной торговли вырос более чем на 20%.

Произошедшие сдвиги, которые будут трансформировать общество еще долгое время после пандемии, предполагают множество позитивных изменений, но благодаря им сбои в сфере кибербезопасности стали главной глобальной угрозой, связанной с технологиями, как отмечено в Докладе Всемирного экономического форума о глобальных рисках за 2021 г. 39% респондентов сочли это «явной и реальной опасностью» для мира в ближайшие два года [1]. В Докладе, по сути, подчеркивается провал мер кибербезопасности в качестве

главного краткосрочного риска: «Меры по обеспечению кибербезопасности бизнеса, правительств и домашних хозяйств стремительно устаревают из-за всё более изощренных и частых киберпреступлений, приводящих к технологическим сбоям, финансовым потерям, геополитической напряженности и социальной нестабильности», – говорится в докладе [1].

Как отмечает журнал Forbes, совокупный ущерб и издержки от киберпреступности гораздо более значительны, чем те, которые причиняются стихийными бедствиями в течение года. Киберпреступность уже стала более прибыльной, чем глобальная торговля всеми основными незаконными наркотиками вместе взятыми.

По мнению исследователей, киберпреступность – это быстро растущая бизнес-модель, поскольку всё более сложное оборудование и объединение преступников в высокоорганизованные банды, работающие по принципам легального бизнеса, делает вредоносные услуги более и доступными для всех, кто хочет нанять киберпреступников.

Cybersecurity Ventures ожидает, что глобальный ущерб от киберпреступности в 2021 г. составит 6 трлн долл. в год (это 16,4 млрд долл. в день, 684,9 млн долл. в час, 11 млн долл. в минуту и 190 тыс. долл. в секунду). Если бы киберпреступность была измерена как страна, она стала бы в этом году третьей по величине экономикой в мире после США и Китая [2].

Киберпреступность развивается стремительными темпами: хакеры и поставщики услуг безопасности непрерывно соперничают, стараясь обойти друг друга, постоянно возникают новые угрозы и инновационные способы борьбы с ними. Перечислим основные тренды в сфере киберпреступности в 2021 г.

Первый тренд – пандемия COVID-19 и переход на удаленный режим работы спровоцировали во всем мире рост числа атак, направленных на эксплуатацию уязвимостей в корпоративных сервисах, доступных из интернета. Пандемия вынудила большинство организаций перевести сотрудников на удаленную работу, часто в достаточно сжатые сроки. Работа на дому создала новые риски, поскольку защита домашних офисов, как правило, гораздо ниже, чем централизованных, которые обычно оснащены сетевыми экранами и маршрутизаторами, а управление доступами регулируется группой кибербезопасности. Переход на удаленную работу осуществлялся в спешке, чтобы не нарушать рабочие процессы, политики кибербезопасности стали более мягкими, а общее количество уязвимостей и поверхности атаки увеличились.

Второй тренд, появившийся на фоне пандемии, – атаки, направленные на кражу учетных данных для подключения к системам аудио- и видеосвязи Skype, Webex и Zoom, а также вмешательство в конференции. Киберпреступники преследовали самые разные цели – от установки майнеров до кибершпионажа в сетях крупных компаний. При этом злоумышленники не ограничиваются одним типом вредоносного ПО: они все чаще используют многофункциональные трояны либо загружают на скомпрометированные устройства набор из различных зловредов.

Самый обсуждаемый тренд в сфере киберпреступности – атаки на интернет вещей. Интернет вещей относится к физическим устройствам, отлич-

ным от компьютеров, телефонов и серверов, которые подключаются к интернету и обмениваются данными. Примеры таких устройств – фитнес-трекеры, умные холодильники, умные часы и голосовые помощники. По оценкам, к 2026 г. в мире будет установлено 64 млрд устройств интернета вещей. Тенденция к удаленной работе способствует увеличению их количества. Большое количество дополнительных устройств меняет динамику и поверхность кибератаки – увеличивается количество потенциальных точек входа для злоумышленников. По сравнению с ноутбуками и смартфонами, устройства интернета вещей имеют меньше возможностей для обработки и хранения данных. Это усложняет использование сетевых экранов, антивируса и других приложений безопасности для их защиты.

Четвертый тренд – рост количества программ-вымогателей. За последние годы атаки вымогателей являются наиболее распространенным типом вредоносного ПО и остаются критической угрозой кибербезопасности, особенно из-за интенсивной цифровизации бизнес-процессов, которую компании прошли или проходят в связи COVID-19. В ходе атаки злоумышленники крадут данные компании, а затем шифруют их, чтобы компания не могла получить к ним доступ. После этого киберпреступники шантажируют компанию раскрытием конфиденциальных данных, если не будет уплачен выкуп. Такие атаки наносят ощутимый ущерб, учитывая конфиденциальность данных, а также экономические последствия уплаты выкупа.

Набирает обороты Big Game Hunting – атаки на крупные компании с целью получения значительного выкупа. Одной из основных движущих сил феноменального роста программ-вымогателей стала модель «Вымогательство как услуга». Ее смысл заключается в том, что разработчики продают или сдают в аренду свои вредоносные программы партнерам для использования в их атаках с целью компрометации сети, заражения и развертывания вымогателей. Вся полученная в виде выкупа прибыль затем распределяется между операторами и партнерами программы.

Хотя в 2021 г. атаке вымогателей подверглись 37% организаций по сравнению с 51% в 2020 г., финансовые последствия атак более чем удвоились, увеличившись за год с 761 тыс. долл. до 1,85 млн долл. [3]. Вероятно, отчасти это связано с переходом злоумышленников к более продвинутым и сложным целевым атакам, от которых труднее оправиться.

По прогнозам, в 2021 г. глобальный ущерб от программ-вымогателей достигнет 20 млрд долл. (рост в 57 раз по сравнению с 2015 г.), а через 10 лет эти убытки превысят невероятные 265 млрд долл. [3].

Пятый тренд – увеличение угроз безопасности облачной инфраструктуры. Уязвимость облачной инфраструктуры остается одной из основных тенденций кибербезопасности. Быстрый повсеместный переход к удаленной работе в период пандемии резко увеличил потребность в облачных сервисах и инфраструктуре, что отразилось на безопасности организаций. Облачные сервисы имеют ряд преимуществ: масштабируемость, эффективность и экономия средств, но в то же время являются основной целью для злоумышленников.

Неверно настроенные параметры облачных сервисов могут стать причиной утечки данных, несанкционированного доступа, небезопасных интерфейсов и взлома учетных записей. Средняя цена утечки данных составляет 3,86 млн долл., поэтому организациям необходимо принять незамедлительные меры по минимизации облачных угроз.

Шестой тренд – рост «умных» атак социальной инженерии. Атаки социальной инженерии, такие как фишинг, не являются новыми, но представляют серьезные угрозы в условиях широко распространившейся в последнее время удаленной работы. Помимо традиционных фишинговых атак на сотрудников, подключающихся к сети работодателя из дома, наблюдется всплеск атак на руководство организации. Рост использования таких приложений для обмена сообщениями, как WhatsApp, Slack, Skype, Signal, WeChat повлек рост популярности SMS-фишинга. Злоумышленники используют эти платформы, чтобы вынудить пользователей загрузить вредоносные программы на свои телефоны.

Седьмой тренд – активное использование искусственного интеллекта для осуществления кибератак. Многие продвинутые вредоносные программы уже ведут себя «умно» – скрытно передвигаются по сетям, сканируют непубличные порты, самостоятельно эксплуатируют огромное количество самых разных уязвимостей, собирают и выводят данные, автоматически определяют нужные им системы. Тем не менее, они не способны к самообучению и самостоятельному расширению собственной функциональности.

А вот использование технологий искусственного интеллекта и машинного обучения в качестве вспомогательного инструмента для автоматизации атак, судя по всему, уже реальность. По данным Европола, на подпольных киберфорумах вовсю обсуждаются, тестируются и даже сдаются в аренду инструменты для взлома паролей и CAPTCHA. Такой инструмент и интересен, и опасен тем, что используемая им нейросеть выстроена по геймификационной модели: за каждую успешную атаку она получает некое вознаграждение и это способствует постепенному развитию её эффективности.

Ожидается, что в ближайшие годы внедрение 5G и технологий искусственного интеллекта позволит проводить атаки, мощность и изощренность которых в десятки и сотни раз превышает возможности киберпреступников сегодня. По прогнозам, с распространением устройств интернета вещей искусственный интеллект совершит в 2040 г. больше киберпреступлений, чем реальные люди.

Восьмой тренд – сегодня в зоне особого внимания хакеров промышленные предприятия и поставщики услуг. В 2020 г. было совершено около 200 атак на энергетические и промышленные компании, когда как годом ранее их было 125. Преступники ориентируются на как можно более крупные организации, в то же время предпочитая придерживаться наименьших затрат на взлом или на покупку готового доступа в инфраструктуру. Повышается и размер выкупов, в отдельных случаях он уже составляет десятки миллионов долларов, но увеличение числа жертв, готовых платить, лишь стимулирует преступников.

Девятый тренд – кибербезопасность обходится государству и бизнес-сообществу всё дороже. Согласно последнему прогнозу Gartner, мировые рас-

ходы на технологии и услуги в области информационной безопасности и управления рисками в 2021 г. вырастут на 12,4% и достигнут 150,4 млрд долл. [4]. Высокие темпы роста отражают сохраняющийся спрос на технологии для дистанционной работы и облачную безопасность. Так, расходы на безопасность облачных сервисов вырастут в 2021 г. на 41,2%. Самую большую категорию расходов (почти 72,5 млрд долл.) представляют услуги в области безопасности, включая консалтинг, аппаратную поддержку, внедрение и аутсорсинговые услуги [4].

Последний из рассмотренных трендов – растущий дефицит кадров в сфере кибербезопасности. Для защиты от хорошо спланированной атаки нужны высококлассные специалисты в сфере кибербезопасности, а их могут себе позволить далеко не все компании. Более того, профессия специалиста в области защиты от киберугроз стала одной из самых дефицитных. По данным Cybersecurity Ventures, в 2021 г. в мире насчитывается 3,5 млн незаполненных вакансий в сфере кибербезопасности [2]. Безработицы в этой области (для опытных работников, а не на должностях начального уровня), начиная с 2011 г., просто не существует. Рост киберпреступности приведет к такому же большому количеству незаполненных должностей в течение следующих 5 лет.

Обозначенные тренды привели к тому, что в настоящее время парадигма кибербезопасности как отдельного предприятия, так и государства в целом меняется в принципе: киберсообщество отказалось от идеи «построения киберзаборов» и пришло к пониманию того, что цель любой системы безопасности состоит в максимально быстром обнаружении атакующего внутри информационных систем.

В течение последнего года пришло понимание, что любая система так или иначе может быть взломана в ходе атаки, и задача главная кибербезопасности – не дать возможности злоумышленнику нанести сколько-нибудь существенный урон работе компании (государственного органа). Эта точка зрения на ситуацию стала в 2020 г. основной и будет оставаться таковой и в ближайшем будущем.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. The Global Risks Report 2021 // WEF [Electronic resource]. URL: https://www.weforum.org/reports/the-global-risks-report-2021. Date of access: 20.11.2021.
2. Morgan, S. Top 5 Cybersecurity Facts, Figures, Predictions, And Statistics For 2021 To 2025 / S. Morgan // Cybercrime Magazine [Electronic resource]. URL: https://cybersecurity ventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/. Date of access: 20.11.2021.
3. The state of ransomware 2021: A Sophos white paper April 2021 // Sophos [Electronic resource]. URL: https://news.sophos.com/en-us/2021/04/27/the-state-of-ransomware-2021/. Date of access: 20.11.2021.
4. Moore, S. Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021 / S. Moore // Gartner [Electronic resource]. URL: https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem. Date of access: 22.11.2021.