ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

ГЕРАСИМОВ Андрей Сергеевич
генеральный директор, ООО «Диджитал Групп», Россия, г. Москва

ОСНОВНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ СЕТЕВОЙ БЕЗОПАСНОСТИ И ВАРИАНТЫ БОРЬБЫ С НИМИ

Аннотация. *Современное глобальное мировое сообщество ставит во главу угла на сегодня сетевую информационную безопасность, что обуславливает необходимость для всех современных компаний обеспечить безопасный доступ каждого сотрудника к сетевым ресурсам в любое время в любом месте. Поэтому в современной стратегии обеспечения сетевой безопасности должны быть учтены такие факторы, как работа по совершенствованию и надежности сетей, продуктивность при реализации управленческих функций безопасностью и осуществление защиты от угроз и атак, которые постоянно эволюционируют и обновляются. Так, для многих отечественных компаний в рамках современной экономической и политической обстановки усложняется обеспечение сетевой информационной безопасности ввиду мобильности сотрудников, использования личных смартфонов, ноутбуков, планшетов и т.д. для работы, что увеличивает количество и качество потенциальных угроз и проблем. Да и хакеры, в свою очередь, создают все более изощренные киберугрозы. Февральские события этого года наложили свой отпечаток на состояние информационной сетевой безопасности: отключение иностранных ИБ-продуктов от обновления и техподдержки, увеличение роста кибератак и т.д. И на уровень вовлеченности в вопрос решения информационной сетевой безопасности любой компании влияет информация, ресурсы и средства защиты непосредственно компании. Поэтому крайне важным является изучение вопроса сетевой безопасности в сложившихся условиях, выявление проблем в этом направлении и вариантов борьбы с ними.*

Ключевые слова. *сетевая безопасность, информационное пространство, кибератаки, киберпространство.*

Ключевым фактором, оказывающим доминирующее влияние на конъюнктуру рынка информационной сетевой безопасности в России в 2022 году, является возросшее в многократном количестве проведение хакерских атак на российские компании, функционирующие в самых разнообразных серах бизнеса. В связи с чем активизировалась позиция государства и регуляторов, что выражается в проведении практической, результативной кибербезопасности в ранг ключевых потребностей. Следующим фактором, не менее радикально трансформирующим рынок, можно назвать практически массовый отток иностранных производителей средств информационной защиты. В этой связи аналитиками производятся постоянные прогнозы, которые на этот год ожидались отрицательными, сокращение объема рынка (объема денег, которые выплачивают клиенты) на 11%; а предварительная оценка Positive Technologies, составленная для рынка информационной сетевой безопасности в нашей стране, - увеличение практически до 20% [5].

Однако в начале следует разобраться с вопросом понятия информационной сетевой безопасности. Сетевая безопасность – ряд вопросов, которые связаны взаимодействием устройств в общей сети, к которым относится, во-первых, защита данных при их передаче посредством линий связи; во-вторых, противодействие несанкционированному удаленному доступу в сеть. Стоит отметить взаимосвязь компьютерной и сетевой безопасности. Под компьютерной безопасностью понимают вопрос защиты данных, которые хранятся, обрабатываются компьютером, выступающим автономной системой [4]. Решение данных вопросов возможно посредством ряда операционных приложений и систем баз данных и

аппаратных средств компьютера. Также стоит акцентировать внимание на том, что также существуют и проблемы, связанные с удаленным входом в сетевые компьютеры, - перехват, анализ сообщений, которые передаются по сети, создание «ложного» трафика.

Отдельно стоит отметить цель кибермошенников. Наиболее интересным предметом для них является то, что подлежит быстрой и легкой монетизации с наименьшими затратами временных и иных ресурсов (аренда сервера, оплата услуг дропперов, курьеров и т.д.). Так, наиболее востребованы для киберпреступников – деньги, которые могут быть у любой компании [1]. Кражу денег кибермошенники могу осуществить у бухгалтера, менеджера, которые ответственны на осуществление платежей и банковских переводов. А в ритейле до денег кибермошенники добираются посредством реализации атак на POS-терминалы. Многие российские компании, банки, относящиеся серьезно к защите своей сетевой безопасности, активам, уже не так интересны злоумышленникам.

Помимо денег популярным для кражи ресурсом остается информация. Она тоже может быть монетизирована. Монетизация бывает нескольких типов: торговля персональными данными клиентов, учетными записями, ключами для расшифровки данных, которые зашифровали злоумышленники [4].

Таким образом, это самые основные проблемы, которые на сегодня являются угрозами для информационной сетевой безопасности, поэтому они требуют определения перспектив их решения.

Как уже говорилось, на сегодня более половины российских компаний практикуют возможность удаленной работы своих сотрудников, однако, важно в тот же момент помнить о том, что присутствует факт недостаточной киберграмотности сотрудников. Удаленная работа обуславливает необходимость удаленного доступа сотрудников к ресурсам компании, однако, не все технологии удаленного доступа достаточно эффективны для защиты информационных активов.

В качестве наглядности можно привести следующий пример. Работая на корпоративном ноутбуке с установленным VPN-клиентом, сотрудник, вводя доменный логин и пароль, имеет доступ к корпоративной сети, к CRM системе компании. При получении фишингового сообщения со ссылкой на страницу, эмулирующую запрос логина и пароля с корпоративной символикой, сотрудник при вводе данных, ничего не подозревая, дает возможность мошенникам доступа к своим учетным данным, к корпоративной сети по VPN, к базе с информацией всей компании. Скопированная база является предметом монетизации для киберпреступников. Такие манипуляции имеют широкое распространение на сегодняшний момент [2].

Для предотвращения подобного возможет перевод доступа пользователей к VPN-шлюзу с доменных логинов и паролей на двухфакторную аутентификацию: первый фактор – сертификат корпоративного устройства, второй – разово сгенерированный временный пароль. Это предотвратит утечку доменного логина и пароля и закроет для мошенников вход в корпоративную сеть через VPN-шлюз. Более серьезным является использование иностранного VPN-инструмента, который на сегодня не обновляется и не поддерживается вендором. Для устранения данной проблемы необходим переход на безопасную настройку с отключением ряда функций либо переход на отечественные аналоги [3].

Еще одной проблемой можно считать неготовность сетевой инфраструктуры компаний к мощным DDoS-атакам. Необходимость в силу специфики компаний доступа ряда сервисов для клиентов в виде веб-сайтов, личных кабинетов, облачных хранилищ требует постоянной и бесперебойной работы этих сервисов, что оказывает непосредственное влияние на финансовое состояние компании. Интересным представляется анализ данных Лаборатории Касперского относительно динамики DDoS-атак на российские организации, что наглядно представлено на диаграмме рисунка 1 [6].

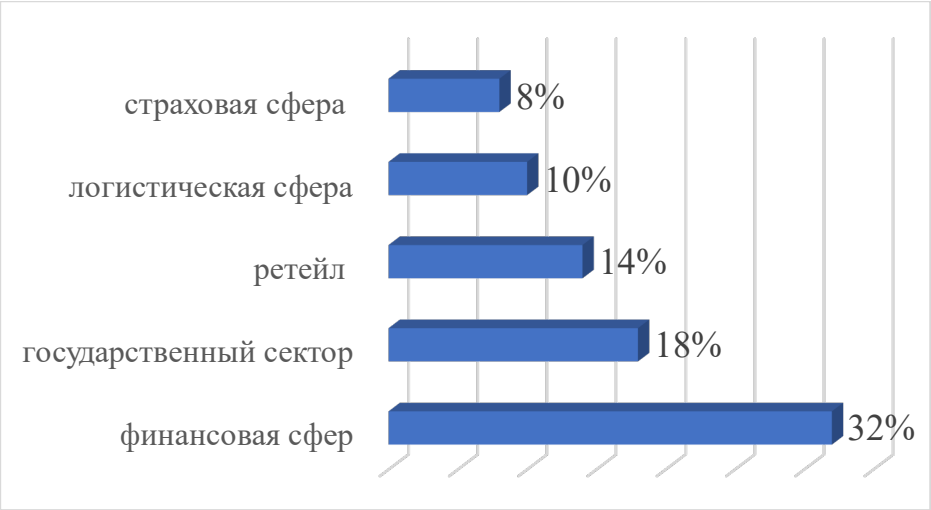

Рис. 1. Наиболее атакуемые отрасли DDoS-атак (% от общего числа атак)

Конечно, на увеличение числа DDoS-атак повлияла напряженность политической ситуации в мире, что обусловила активность так называемых хактивистов, целью которых является нанесение вреда экономике и социальной сфере России. Многие компании оказались бессильны противостоять этим атакам, так как мощность некоторых доходит до десятков гигабит/сек. Зафиксировано самое длительное время DDoS-атаки, которая составляла 145 часов [6].

В качестве наглядного примера данной проблемы можно привести функционирование web-сайта и почтового сервера сетевого ретейлера, которые были установлены на физических серверах в сетевом периметре компании, которая подверглась мощной DDoS-атаке. Это обусловило отсутствие доступа для пользователей практически на сутки, в течение которых была произведена атака по перебору паролей пользователей по заранее добытой адресной книги компании на страничку входа в Outlook Web App [6]. Отдельно стоит отметить, что, согласно политике компании, 5 неправильных попыток ввода логина и пароля обуславливают блокировку учетной записи, что, собственно, и повлекло за собой блокировку практически всех учетных записей работников компании, что принесло убытки в размере суточного объема продаж для компании и дневной заработной платы для работников.

Для предотвращения подобного возможно использование специализированных аппаратных средств для защиты от DDoS и brute force (перебор пароля) атак, например решения класса WAF), либо использование облачных решений, либо расширить пропускную способность сети и т.д.

Можно привести еще ряд примеров нарушения сетевой информационной безопасности. Приведенные же примеры демонстрируют то, что от уровня проработки сетевой архитектуры зависит общая успешность мер защиты. Ведь примерно 90% взаимодействий злоумышленников в рамках атаки происходит через сеть, а большинство международных производителей средств защиты от сетевых угроз отказались от продажи и поддержки своих продуктов для российских организаций, к тому же найти в штат специалистов, имеющих необходимый опыт, знания и компетенции для перевода сетевой инфраструктуры с зарубежных аналогов на российские продукты довольно непросто [6].

На схеме рисунка 2 представлены средства и способы информационной сетевой защиты [4].

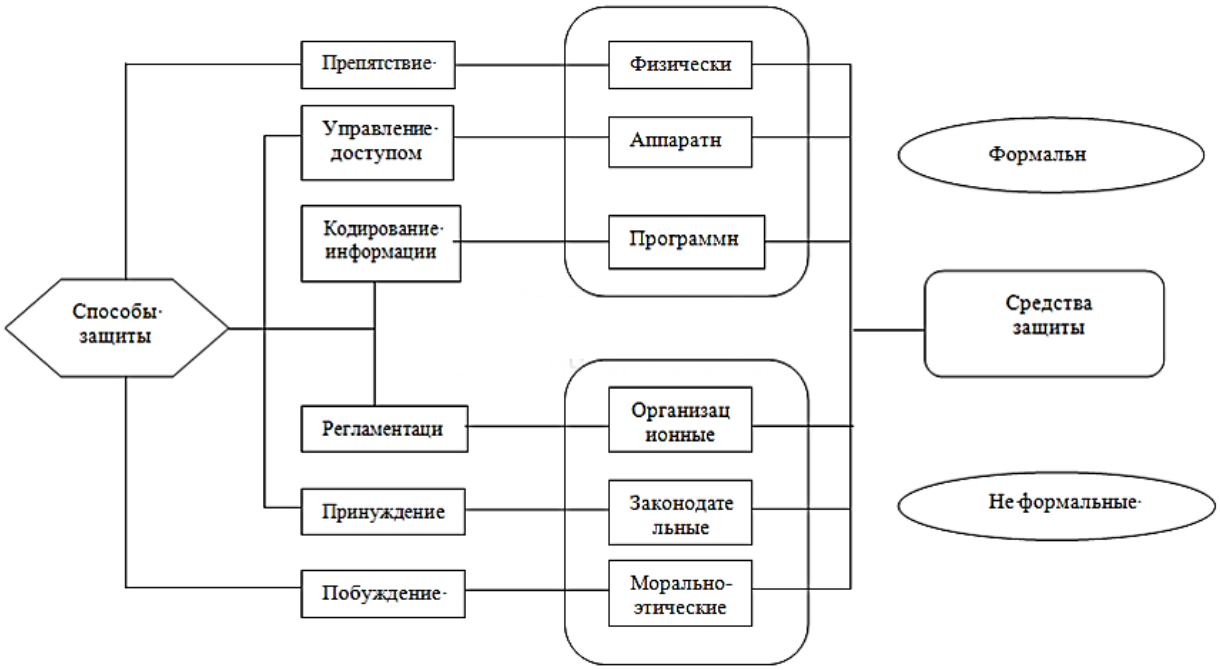

Рис. 2. Средства и способы информационной сетевой защиты

Тем не менее задача по обеспечению аналогичного уровня сетевой безопасности на основе российских решений, является одной из актуальных на данный момент, что сделает процесс взлома для злоумышленника настолько трудоемким, чтобы ему было невыгодно тратить столько ресурсов. Киберпреступники постоянно повышают уровень своей «квалификации», тем самым увеличивая количество собственных преступлений. Поэтому отечественные компании должны минимизировать риски, не только задействовать уже имеющиеся методы безопасности, но и работать над постоянным внедрением передовых технологий защиты.

Сложившаяся на сегодня политическая и экономическая ситуация для нашей страны проявила вектор перемещения компаний на российские программные продукты, операционные системы, что, в свою очередь, оказало значительное влияние на поддержку российских ОС вендорами ИБ. Так, например, большая часть продуктов Positive Technologies еще в 2022 году начала поддерживать ОС Astra Linux, в 2023 году продолжится развитие в этом направлении, а добавление и других отечественных ОС [5]. В свою очередь, рассмотренное выше демонстрирует тот факт, что наступивший 2023 год станет стартовым для разработки новых, и главное, российских, технологических решений, которые ранее были не такими актуальными и значимыми по своим масштабам.

Литература

1. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт. Монография. Гриф УМЦ «Профессиональный учебник». Гриф НИИ образования и науки. / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИ, 2016. – 239 с.

2. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. – М.: ГЛТ, 2016. – 280 с.

3. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. – М.: МГИУ, 2017. – 277 с.

4. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: Форум, 2018. - 256 с.

5. Официальный сайт Positive Technologies [электронный источник]. Режим свободного доступа. https://www.ptsecurity.com/ww-en/ (дата обращения 03.02.2023)

6. Официальный сайт «Лаборатория Касперского» [электронный источник]. Режим свободного доступа. https://www.kaspersky.ru/ (дата обращения 03.02.2023)

GERASIMOV Andrey Sergeevich
General Director of Digital Group LLC, Moscow, Russia

THE MAIN PROBLEMS OF INFORMATION NETWORK SECURITY AND OPTIONS FOR DEALING WITH THEM

Abstract. *The modern global world community puts network information security at the forefront today, which makes it necessary for all modern companies to ensure safe access of each employee to network resources at any time, anywhere. Therefore, the modern strategy of ensuring network security should take into account such factors as the work on improving and reliability of networks, productivity in the implementation of security management functions and the implementation of protection against threats and attacks that are constantly evolving and updated. Thus, for many domestic companies, within the framework of the modern economic and political situation, it is becoming more difficult to ensure network information security due to the mobility of employees, the use of personal smartphones, laptops, tablets, etc. for work, which increases the number and quality of potential threats and problems. And hackers, in turn, create increasingly sophisticated cyber threats. The February events of this year have left their mark on the state of information network security: the disconnection of foreign information technology products from updates and technical support, an increase in the growth of cyber attacks, etc. And the level of involvement in the issue of solving the information network security of any company is influenced by the information, resources and means of protection of the company itself. Therefore, it is extremely important to study the issue of network security in the current conditions, identify problems in this direction and options to combat them.*

Keywords: *network security, information space, cyber attacks, cyberspace.*