Кибератака как новый вид чрезвычайных ситуаций

Н.Н. Чибинев, Н.В. Ляшенко

Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова, Новочеркасск

Аннотация: Проблема информационной безопасности подробно исследуется с учетом последствий кибератак на технологические системы. Использовались методы обобщения, обработки и анализа статистических данных о чрезвычайных ситуациях, причинами которых стали кибератаки. Научные методы исследования концентрировались на выявлении ключевых причин «успешных» хакерских атак и оценке эффективности технологических методов в обеспечении информационной безопасности. Показаны принципиальные проблемные вопросы, возникшие у IT- специалистов по принятию, реализации и развитию термина и понятия «киберчрезвычайная ситуация», сформулировано его определение. Проведённые исследования обуславливают необходимость постоянного развития методов и стратегий обеспечения информационной безопасности, а также формирования законодательных актов о порядке объявления чрезвычайной ситуации при совершении кибератак.
Ключевые слова: кибербезопасность, киберчрезвычайная ситуация, мониторинг безопасности, модель Zero Trust, киберстрахование.

Глобальная компьютеризация жизнедеятельности в мире вызывает ежегодно лавину кибератак. Немецкий веб-портал «sicherheitstacho.eu» установил, что ежесуточный рост идентифицированных кибератак в мире приобрёл глобальный характер и составляет более 40 млн, при этом финансовые потери от них в 2022 году оцениваются в 8 трлн. долларов, что значительно больше убытка от пандемии COVID-19 [1,2]. По прогнозам зарубежных исследователей ущерб от киберпреступности к 2025 году составит сумму 10,5 триллионов долларов [3].

В нашей стране кибератаки происходят во всех сферах деятельности человека и направленны в основном на подрыв безопасности объектов экономики [4, 5] и информационных систем государственных учреждений (табл.1). Вице-премьер РФ Чернышенко Д.Н. 6 февраля 2024 года, выступая на форуме "Цифровая экономика" в рамках выставки "Россия", сообщил, что в 2023 году российские IT-специалисты отразили более 65 тыс. кибератак на критическую информационную инфраструктуру. При этом следует отметить,

что в 2021 г. целью атак был финансовый сектор, а в 2022 г. – государственный сектор [6]. В последние два года ИБ-центр ФСБ регистрирует более 170 кибератак каждый день. Ещё в 2013году министр обороны России генерал армии Шойгу С.К. сравнил киберугрозы с оружием массового поражения.

Таблица 1

Кибератаки в Российской Федерации январь 2022 -октябрь 2023гг

№ п/п	Кибератакуемые отрасли экономики России	Доля кибератак, %
1	Государственный сектор	43
2	Телекоммуникации	14
3	Сельское хозяйство	9
4	Финансовый сектор	7
5	Промышленность	7
6	Сфера услуг	4
7	Ритейл	4
8	Образовательный сектор	4
9	Некоммерческие организации (НКО)	4
10	Энергетика	4

Кибератаки в настоящее время становятся самыми распространёнными причинами возникновения различных видов преступлений [7], не редко приводящих к чрезвычайным ситуациям. Характерными примерами о возможности возникновения техногенных и социальных чрезвычайных ситуаций от кибератак могут служить события в ряде регионов нашей страны. В марте 2022 года кибератакам подвергались агрохолдинг «Мираторг» и «Ростовский колбасный завод – ТАВР» в следствии чего 18 предприятий агрохолдинга не могли оформлять производственные, транспортные и ветеринарные документы на продукцию и была временно остановлена работа завода «Тавр» в Ростовской области. 22 и 28 февраля 2023 года из-за хакерской атаки на сервера радиостанций в Казани, Уфе, Белграде, Нижнего Новгорода, в Крыму и других городах неоднократно звучала в эфире этих радиостанций ложная информация об объявлении

воздушной тревоги. В этой связи МЧС России перенесла комплексные проверки систем оповещения населения на территории страны с 1 марта на 4 октября 2023 год. Однако, как показывает практика в нашей стране, при совершении кибератак режим чрезвычайной ситуации, связанной с ликвидаций возникших последствий на объектах и территориях, не объявляется, хотя прямые и косвенные убытки от них всегда значительные и последствия устраняются продолжительный период времени.

В мире есть примеры объявления режима ЧС при кибератаках на компьютерные сети организаций и объекты экономики. Так 13декабря 2019 года мэр города Новый Орлеан США Латоя Кантрелл объявила режим ЧС из-за кибератаки на городскую телефонную сеть. В результате проведенной компьютерной атаки 7 мая 2021 года на один из крупнейших трубопроводных операторов в США – Colonial Pipeline Company, снабжающая топливом 50 миллионов американцев, совершена кибератака. Администрация президента и Минтранс США объявили, что в 17 штатах страны о введении режима региональной чрезвычайной ситуации. Введение режима, осуществлено для создания условий немедленной транспортировки бензина, авиационного керосина, дизельного топлива и иных очищенных нефтепродуктов 45% потребителям страны. 6 июля 2021 года власти округа Анхальт- Биттерфельд (земля Саксония- Анхальт на востоке Германии) ввели режим чрезвычайной ситуации из-за хакерской атаки на районные компьютерные сети.

Особенностью чрезвычайных ситуаций информационного характера является скорость их распространения. Она может быть, как внезапная, так и по происшествии некоторого времени. То есть, разрушающее программное средство может существовать в компьютерной системе, не проявляя себя, до наступления определённого события, даты или свершения определённого действия, а может быть спрограммировано так, что причинит вред сразу с

момента проникновения в систему. До того, как разрушающее программное средство себя проявит, логику его действий предсказать весьма трудно.

Это подчеркивает опасность киберугроз, как потенциальных чрезвычайных ситуаций. Для борьбы с ними необходимо разработать нормативно-законодательные документы и использовать современные технологические решения. На государственном уровне в России в настоящее время общепринятого понимания «киберчрезвычайной ситуации» не существует, кроме этого до настоящего времени в научном сообществе ведется дискуссионное обсуждение понятий терминов «кибератака и кибербезопасность» [8], хотя они установлены в ГОСТ Р 56205-2014 и ГОСТ Р 56498-2015, а в Уголовном Кодексе РФ предусмотрены статьи 272-274 за преступления в сфере компьютерной информации.

Целью проведённого исследования является акцентирование внимания на необходимости введения понятия кибератаки, как чрезвычайной ситуации и анализ технологических аспектов обеспечения информационной безопасности на объектах экономики и организациях с акцентом на шифрование данных и коммуникаций, аутентификацию и авторизацию, мониторинг и анализ безопасности, а также защиту от вредоносных программ.

Данная проблема рассматривалась с точки зрения предупреждения киберчрезвычайных ситуаций в технологических процессах производства и в различных сферах общественной жизни. Для решения поставленной задачи были обобщены, обработаны и проанализированы статистические данные о чрезвычайных ситуациях от кибератак и утечек данных в целом по России на различных производственных объектах и организациях. В процессе отбора статистических данных использовались методы, как сплошного, так и выборочного исследования.

При мониторинге и анализе кибератак установлено, что у IT-специалистов сформировались принципиальные проблемные вопросы по принятию, реализации и развитию термина и понятия «киберчрезвычайная ситуация», связанные с тремя основными причинами:

- установление дополнительных финансовых затрат для IT- компаний;

- установление излишних бюрократических барьеров для IT-компаний с целью выявления потенциального источника (атрибуции) кибератак;

- возложение ответственности за происшедшую кибератаку в организации или на объекте экономики на IT- специалистов данных объектов.

Кроме этого, отрицание введения термина и понятия «киберчрезвычайная ситуация» обосновывается опасением необходимости разработки новой нормативно-методической базы и новых национальных стандартов в части пожарной, промышленной, экологической и кибербезопасности.

В ходе исследования был проведен анализ последствий кибератак, нацеленных на технологические системы производственных объектов, который выявил следующие типичные уязвимости и уровни защиты, которые были нарушены: не обновляемые устройства, устаревшие системы и ПО, слабые аутентификационные меры, и недостаточная сетевая сегментация.

Анализ кибератак показал основные типы кибератак [9,10]: вредоносное программное обеспечение (трояны, сетевые черви, вирусы), DoS- и DDoS-атаки, фишинг, SQL-инъекции, XSS, ботнеты, брутфорс-атаки, MITM, «Щенки PUPS» и социальная инженерия.

Исследование установило несколько основных причин, по которым «успешные» кибератаки на технологические системы производственных объектов становились возможными: недостаточное осознание рисков,

отсутствие системы мониторинга и реагирования, недостаточное внимание к персоналу и неактуальные политики безопасности

Данный анализ кибератак позволил определить современную базовую модель термина «киберчрезвычайная ситуация», которая должна в своём составе не только отражать и соответствовать классической терминологии, изложенной в федеральном законе от 21.12.1994 №68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера», а также ГОСТ Р 22.0.02-2016, ГОСТ 22.0.03-2022, ГОСТ Р 22.0.05-2020 и ГОСТ Р 22.0.04-2020, но и содержать требования нормативно-правовых документов по кибербезопасности. Таким образом, общее определение киберчрезвычайной ситуации может выглядеть так:

Киберчрезвычайная ситуация – это обстановка на конкретных объектах жизнедеятельности или определённой территории, сложившаяся в результате разрушения их компьютерно-телекоммуникационной инфосферы, повлекшие за собой ущерб здоровью людей или окружающей среде, приостановку производственной деятельности, значительные материальные потери и нарушение условий жизнедеятельности людей.

Для достижение целей защиты от киберугроз необходимо:

1. Внести в единые нормативно-законодательные акты по безопасности в системе МЧС России понятие о киберчрезвычайной ситуации и порядок её установления и классификации. Термин «киберчрезвычайная ситуация» должен выступить как фактора, снижающий социальное напряжение и предписывающий соответствующие законодательные меры по локализации последствий от данного вида чрезвычайной ситуации.

2. Выполнить Указ Президента Российской Федерации №166 от 30.03.2022 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» с 1 января 2025 года не допускать использование иностранного

программного обеспечения на объектах критической инфраструктуры, принадлежащей госорганам.

3. Использовать наиболее эффективный в настоящее время способ обеспечения информационной безопасности – модель Zero Trust, включающая в себя многие слои аутентификации, мониторинг сетевого трафика, криптографию и анализ поведения пользователей. Для реализации концепции Zero Trust используется шлюз кибербезопасности NGFW (Next-Generation Firewall) и применяются классические продукты класса IDM (Identity and Access Management), PAM (Privileged Access Management), EDR (Endpoint Detection and Response) и DLP (Data Loss Prevention).

4. Развивать рынок киберстрахования в России, как один из видов комплексной защиты от всевозможных киберугроз.

5. Методы и решения обеспечения и управления информационной безопасности составляют только один из элементов в общей стратегии обеспечения безопасности объектов экономики и организаций, при этом необходимо организовывать постоянное обучение сотрудников по вопросам кибербезопасности.

6. Для эффективного обеспечения безопасности компьютерных систем необходимо сформировать для объектов экономики и организаций модель угроз технологической безопасности программного обеспечения – официально принятый корпоративный нормативно-технический документ, которым обязаны руководствоваться заказчики и разработчики программных комплексов.

7. Из-за отсутствия международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, назрела острая необходимость принятия специального международного законодательного документа, определяющего правовые и организационные основы борьбы с чрезвычайными ситуациями информационного характера.

Литература

1. Резниченко Л.С. Современные и перспективные угрозы информационной безопасности // Научные труды КубГТУ. 2023. №3. С. 80-92.

2. Goel S., Nussbaum B. Attribution Across Cyber Attack Types: Network Intrusions and Information Operations // IEEE Open Journal of the Communications Society. 2021. №2. pp. 1082-1093.

3. Morgan S. 2021 report cyberwarfare in the c-suite // Cybercrime facts and statistics. 2021. Jan. 21. 19 p.

4. Ибрагимова З.М., Батчаева З.Б. Информационная безопасность как элемент экономической безопасности // Инженерный вестник Дона, 2022, №11. URL: ivdon.ru/ru/magazine/archive/n11y2022/8010.

5. Lapshina I.V., Kravets A.V. Modern cybersecurity from the perspective of cognitive modeling // Инженерный вестник Дона, 2023. №1. URL: ivdon.ru/ru/magazine/archive/n1y2023/8120.

6. Бутырский И.Ф., Петрищев Н.В. Кибератаки на сайты организаций, сигнатурный анализ этих атак и противодействие им // Наука, техника и образование. 2023. № S1(41). С. 32-41.

7. Кобец П.Н. Киберпреступность: современные виды, причины, ее порождающие, и особенности предупреждения // Вестник Самарского юридического института. 2022. №1(47). С. 52-58.

8. Шинкарецкая Г.Г. Проблема выработки определения кибератаки // Международное право. 2023. №2. С. 10-21.

9. Кулагина И.И., Семикин Д.В. Феномен кибератак: причины, последствия, способы противодействия (на примере зарубежного опыта) // Теория и практика общественного развития. 2022. №12(178). С. 51-56.

10. Кобец П.Н. Киберпреступность: современные виды, причины, ее порождающие, и особенности предупреждения // Вестник Самарского юридического института. 2022. №1(47). С. 52-58.

References.

1. Reznichenko L.V. Nauchnye trudy Kubanskogo gosudarstvennogo tekhnologicheskogo universiteta. 2023. №3. pp. 80-92.

2. Goel S., Nussbaum B. IEEE Open Journal of the Communications Society. 2021. №2. pp. 1082-1093.

3. Morgan S. Cybercrime facts and statistics. 2021. Jan. 21. 19 p.

4. Ibragimova Z.M., Batchaeva Z.B., Батчаева З.Б. Inzhenernyi vestnik Dona, 2022, №11. URL: ivdon.ru/ru/magazine/archive/n11y2022/8010.

5. Lapshina I.V., Kravets A.V. Inzhenernyi vestnik Dona, 2023. №1. URL: ivdon.ru/ru/magazine/archive/n1y2023/8120.

6. Butyrsky I.F., Petrishchev N.V. Nauka, tekhnika i obrazovanie. 2023. № S1 (41). pp. 32-41.

7. Kobets P.N. Vestnik Samarskogo yuridicheskogo instituta. 2022. №1 (47). pp. 52-58.

8. Shinkaretskaya G.G. Mezhdunarodnoe pravo. 2023. №2. pp. 10-21.

9. Kulagina I.I., Semikin D.V. Teoriya i praktika obshchestvennogo razvitiya. 2022. №12(178). pp. 51-56.

10. Kobets P.N. Vestnik Samarskogo yuridicheskogo instituta. 2022. №1 (47). pp. 52-58.

Дата поступления: 3.05.2024
Дата публикации: 25.06.2024