конфликтами на международном уровне для повышения их эффективности и стабильности.

Источники

1. В Генассамблее ООН обсудили вопрос применения Россией права вето при голосовании по трансграничному механизму в Сирии // Организация объединенных наций. – URL: <https://news.un.org/ru/story/2023/07/1443002> (дата обращения: 19.07.2023).

2. Миссия Организации Объединенных Наций в Южном Судане [сайт]. – Нью-Йорк, 2024. – URL: <https://unmiss.unmissions.org/> (дата обращения: 19.11.2024).

3. Миссия Организации Объединенных Наций по содействию Афганистану [сайт]. – Нью-Йорк, 2024. – URL: <https://unama.unmissions.org/> (дата обращения: 19.11.2024).

4. Миссия Организации Объединенных Наций по стабилизации в ДР Конго [сайт]. – Нью-Йорк, 2024. – URL: <https://monusco.unmissions.org/> (дата обращения: 19.11.2024).

5. UN resolutions 1970 & 1973 // Temehu. – URL: <https://www.temehu.com/un-resolutions-1970-1973.htm> (date of access: 19.11.2024).

6. 2023 corruption perception index // Transparency international. – URL: <https://www.transparency.org/en/cpi/2023/index/afg> (date of access: 30.01.2024).

***Б.И. Шумская**, магистрант*

*Научный руководитель – Н.Ю. Веремеев, кандидат политических наук
БГЭУ (Минск)*

СОВРЕМЕННЫЕ ИТ-РЕШЕНИЯ ДЛЯ ЗАЩИТЫ КРИТИЧЕСКИ ВАЖНОЙ ИНФРАСТРУКТУРЫ ГОСУДАРСТВА ОТ КИБЕРТЕРРОРИЗМА

Если XX в. еще можно охарактеризовать с политической точки зрения – веком войн, тоталитаризма и традиционного терроризма, то XXI в. описывается таким понятием как «кибертерроризм». Кибертерроризм – это особая форма терроризма, глубоко интегрированная в цифровую среду. Она представляет собой конвергенцию терроризма и киберпространства. Компьютерные технологии выступают как объект и средство атаки. Объект атак обычно представлен информационными сетями критически важной инфраструктуры, системами управления промышленными процессами (SCADA-системы), персональными компьютерами и мобильными устройствами граждан. Средствами осуществления атак выступают вредоносные программные

обеспечения (вирусы, трояны, ботнеты), инструменты для взлома и несанкционированного доступа к информационным системам.

Возрастающая кибернетическая угроза создает существенный риск для функционирования критически важной инфраструктуры государства. Поэтому исследование современных ИТ-решений для обеспечения ее информационной безопасности является крайне актуальным. Целью данной статьи является систематизированный анализ и обзор эффективных технологий и методов защиты от кибератак.

Отличие кибертерроризма от традиционного терроризма заключается в его способности наносить ущерб критически важной инфраструктуре в кратчайшие сроки. Критически важная инфраструктура государства (КВИГ) часто определяется как инфраструктура, неправильное функционирование которой в течение ограниченного периода времени, может негативно повлиять на экономику отдельных субъектов, повлечь за собой финансовые потери или подвергнуть людей риску безопасности [5, с. 5–6]. Ее составляющие – узловые сектора для поддержания национальной безопасности, экономического благополучия и социального порядка. К ним относятся: энергетика (электростанции, линии электропередач, газо- и нефтепроводы), транспорт (железные дороги, аэропорты, морские порты), здравоохранение (больницы, фармацевтические предприятия), финансы (банковская система, платежные системы), телекоммуникации (связь, интернет-провайдеры), водоснабжение. Взаимозависимость элементов КВИГ делает ее уязвимой для каскадных сбоев, при которых атака на один компонент вызывает цепную реакцию, и парализует всю систему.

Квалифицированное действие кибертерроризма характеризуется четырьмя взаимосвязанными элементами: применением компьютерных технологий, политической мотивацией, физическим насилием и воздействием на психику населения. К проявлениям кибертерроризма относятся дезинформационные кампании, атаки на государственные информационные системы, финансовые махинации и хищение конфиденциальных данных [1, с. 211–212].

Для эффективной защиты КВИГ требуются современные ИТ-решения, учитывающие указанные векторы угроз. Расширенная система обнаружения и предотвращения вторжений (IDS/IPS) обеспечивает мониторинг сетевого трафика и выявление подозрительной активности. Использование машинного обучения в современных ИТ-решениях повышает точность обнаружения. В качестве примеров актуальных программных решений можно привести Snort, Zeek и Suricata, каждая из которых обладает специфическими преимуществами и функциональными особенностями.

Snort – система, использующая сигнатурный и аномальный анализ трафика. При обработке больших объемов данных она нуждается в регулярном обновлении для эффективного обнаружения новых угроз [6]. Система Zeek (Bro)

обеспечивает детальный анализ сетевого трафика. Выявляет поведенческие аномалии и предоставляет подробные данные для реагирования на инциденты. Данная система требует высокой квалификации персонала для эффективного использования [8]. Suricata – высокопроизводительная система обнаружения вторжений, эффективно использующая ресурсы и сочетающая сигнатурный и аномальный анализ. Баланс производительности и точности делает ее привлекательным ИТ-решением для защиты критически важной инфраструктуры государства [7]. Выбор IDS/IPS зависит от требований, объема трафика, ресурсов и квалификации. Комбинированный подход используется эффективнее.

Использование интеграции многофакторной аутентификации (MFA) и искусственного интеллекта (ИИ) создает многоуровневую систему информационной защиты критически важной инфраструктуры. MFA добавляет дополнительный уровень безопасности для проверки личности пользователей. ИИ обеспечивает активное обнаружение и реагирование на угрозы. Минимизируются риски в условиях эволюционирующего киберландшафта.

Следует иметь в виду, что человеческий фактор остается первостепенной уязвимостью критической инфраструктуры. Регулярное обновление знаний и практическая отработка навыков персонала гарантирует соответствие нормативным требованиям и уменьшит количество инцидентов. В XXI в. инвестиции в программы повышения информационной грамотности становятся экономически оправданными.

Защита конфиденциальности данных в государственных структурах имеет второстепенное значение. Это обусловлено рядом факторов: недостаточное финансирование, отсутствие оптимально разработанной нормативно-правовой базы и нехватка квалифицированных специалистов в области защиты информации. Утечки данных чреваты серьезными последствиями, поэтому необходимы строгие меры. К примеру, внедрение протоколов шифрования в целях защиты данных при передаче и хранении. Ограничение доступа к конфиденциальной информации только для уполномоченного персонала. Проведение регулярных аудитов для выявления уязвимостей данных.

Парадокс заключается в том, что несмотря на признание человеческого фактора как основной уязвимости критической инфраструктуры, защита конфиденциальности данных в государственных структурах остается недостаточной. Это кажущееся противоречие можно объяснить с помощью нескольких научных подходов. Теория институциональной экономики опирается на асимметрию информации между гражданами (принципалами) и чиновниками (агентами), которая ведет к несоответствию интересов и слабой подотчетности [3, с. 275–276]. Возникает проблема коллективных действий, где отсутствие координации между ведомствами препятствует эффективной защите данных. В результате, институциональная интервенция проявляется

в сопротивлении изменениям. Бюрократические барьеры замедляют процесс внедрения современных мер кибербезопасности.

Согласно теории организационного поведения, когнитивные искажения влияют госслужащих и индивидов в целом. Данные искажения основываются на переоценке собственных способностей и недооценке рисков. Вследствие этого, эволюция новейших методов защиты стоит на месте [2, с. 17–18].

Таким образом, непредсказуемость, анонимность и практическая невозможность предотвращения кибертерактов делает их чрезвычайно действенным способом борьбы. Исход атак практически не зависит от того, в каком состоянии находятся экономика и вооруженные силы государства. Два фактора могут ограничивать потенциал кибертеррористов.

Во-первых, отсутствие общественной поддержки. Распространение информации о кибератаках и их последствиях будет затруднено. Неприятие обществом целей кибертеррористов делает атаки менее успешными, усложняет достижение политических или иных целей. Повышение информационной грамотности населения и пропаганда гражданской ответственности являются важнейшими мерами противодействия.

Во-вторых, эффективность государственной системы кибербезопасности. Превентивные меры защиты, оперативное обнаружение и реагирование на инциденты становятся во главе сильной системы информационной безопасности КВИГ. Строгое правоприменение создает сдерживающий эффект воздействия на кибертерроризм. В таком случае, анонимность киберпреступников не гарантирует безнаказанность. Система предотвращения, расследования и наказания снижает привлекательность кибертеррористической деятельности и ограничивает ее масштабы.

Абсолютная информационная безопасность недостижима. Непрерывное совершенствование систем защиты и повышение уровня цифровой грамотности населения являются необходимыми условиями минимизации рисков кибертерроризма.

Источники

1. Драгун, Д. В. Кибертерроризм – новая и наиболее опасная форма терроризма в условиях цифровизации Белорусского государства / Д. В. Драгун / У истоков и в авангарде белорусской политологии : материалы науч. конф., посвящ. 30-летию кафедры политологии Белорус. гос. ун-та, Минск, 27 нояб. 2020 г. / Белорус. гос. ун-т ; редкол.: Н. А. Антанович (гл. ред.) [и др.]. – Минск, 2020. – С. 209–214.

2. Кашапова, Э. Р. Когнитивные искажения и их влияние на поведение индивида / Э. Р. Кашапова, М. В. Рыжкова // Вестн. Томск. гос. ун-та. – 2015. – Т. 30, № 2. – С. 15–26.

3. Силова, Е. С. Проблема преодоления информационной асимметрии в государственном управлении / Е. С. Силова, Е. Е. Ковина // Вестн. Челяб. гос. ун-та. – 2023. – Т. 478, № 8. – С. 274–282.

4. Cybersecurity solutions for critical infrastructure // Ana Crudu and MoldStud research team. – URL: <https://moldstud.com/articles/p-cybersecurity-solutions-for-critical-infrastructure> (date of access: 19.11.2024).

5. Critical infrastructure protection: threats, attacks and countermeasures / R. Baldoni [et.al.]. – Rome : Center of Cyber Intelligence and Information Security, 2014. – 170 p.

6. Snort – Network Intrusion Detection and Prevention System. – URL: <https://snort-org.herokuapp.com/> (date of access: 11.11.2024).

7. Suricata. – URL: <https://suricata.io/> (date of access: 13.11.2024).

8. Zeek – The Zeek Network Security Monitor. – URL: <https://zeek.org/> (date of access: 12.11.2024).