PISA
Platforma pentru Inițiative de Securitate și Apărare

DCAF Geneva Centre for Security Sector Governance

Sweden
Sverige

Динамика кибербезопасности в Республике Молдова: ответ на сложные угрозы

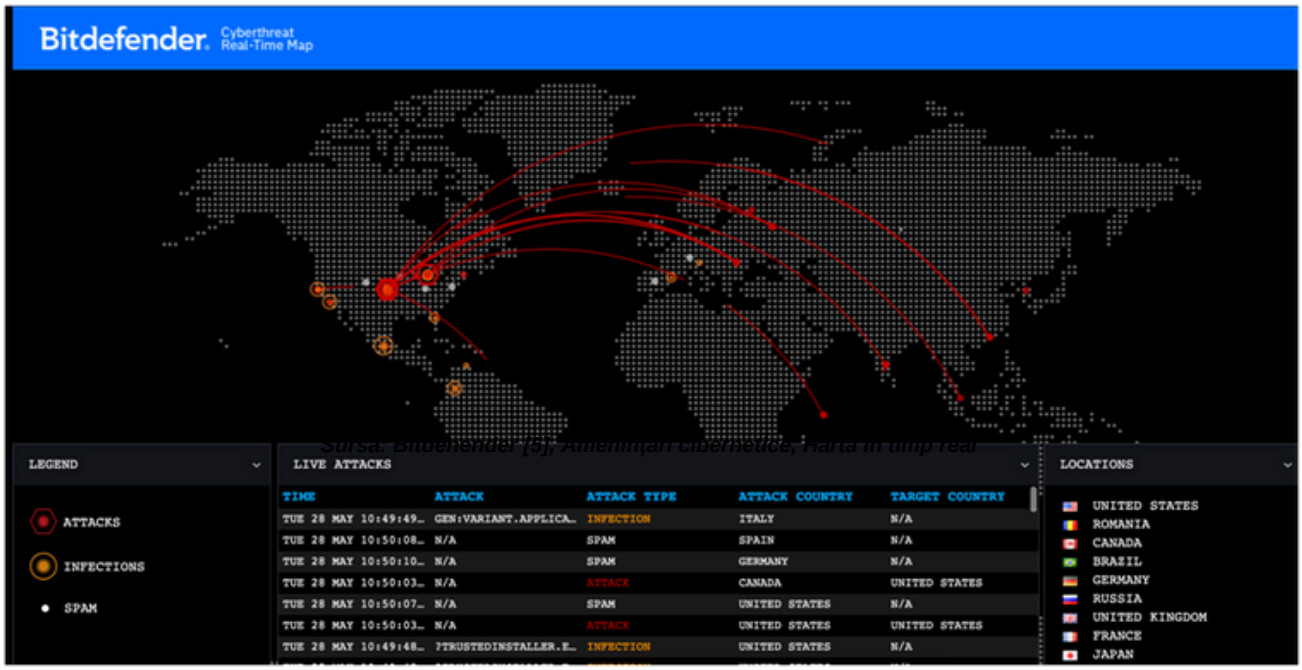
Санда САНДУ,
Эксперт в области безопасности и политики хорошего управления

МАТЕРИАЛ РАЗРАБОТАН В КОНТЕКСТЕ ПРОЕКТА "ИНФОРМАЦИОННАЯ КАМПАНИЯ ПО ЗАДАЧАМ ПОЛИТИК В ОБЛАСТИ БЕЗОПАСНОСТИ В РЕСПУБЛИКЕ МОЛДОВА", РЕАЛИЗУЕМОГО ПЛАТФОРМОЙ ПО ИНИЦИАТИВАМ В ОБЛАСТИ БЕЗОПАСНОСТИ И ОБОРОНЫ (ПИСА) И ПОДДЕРЖИВАЕМОГО ЖЕНЕВСКИМ ЦЕНТРОМ ПО УПРАВЛЕНИЮ СЕКТОРОМ БЕЗОПАСНОСТИ (DCAF), В РАМКАХ ПРОЕКТА "УКРЕПЛЕНИЕ УПРАВЛЕНИЯ СЕКТОРОМ БЕЗОПАСНОСТИ В МОЛДОВЕ", ФИНАНСИРУЕМОГО ШВЕЦИЕЙ.

Кибербезопасность - это деятельность или процесс, способность, возможность или состояние, с помощью которых информационные и коммуникационные системы, поддерживающие или влияющие на результаты развития, а также содержащаяся в них информация, защищены от повреждений, несанкционированного использования, изменений или эксплуатации.

В эпоху цифровых технологий кибербезопасность стала важным аспектом национальной и международной безопасности. Кибербезопасность включает в себя комплекс мер и практик, направленных на защиту информационных систем, сетей и данных от несанкционированного доступа, злоупотребления, утечки, нарушений, изменений или уничтожения. Это мультидисциплинарная область, требующая сотрудничества между правительствами, частным сектором и гражданами для обеспечения безопасной и надежной цифровой среды.
Ландшафт киберугроз динамичен и постоянно развивается. Он включает в себя широкий спектр атак и техник, используемых злонамеренными акторами, включая:

- **Фишинговые атаки.** Мошеннические электронные письма и сообщения, направленные на получение чувствительной информации, такой как пароли и банковские данные, путем обмана пользователей. По данным от PhishMe, 91% всех кибератак начинаются с фишинговых писем. [1].
- **Вымогательство (Ransomware).** Вредоносное программное обеспечение, которое шифрует данные жертв и требует выкуп за их расшифровку. Согласно данным Cybersecurity Ventures, глобальные затраты на киберпреступность оцениваются в 9,5 трлн долларов США в год к 2024 году [2]. К этому добавляются растущие затраты на ущерб, причиненный киберпреступностью, которые ожидается что достигнут 10,5 трлн долларов США к 2025 году.
- **DDoS-атаки (Distributed Denial of Service).** Заполнение сервера или сети избыточным трафиком для их недоступности. DDoS-атаки продолжают увеличиваться по размеру и сложности и 2023 год ускорил эту тенденцию в неожиданном темпе. Геополитика стала ключевым фактором роста DDoS-атак. Мы видели, [3] как атаки усилились в странах как США, Россия, Украина, Израиль, Германия, Франция, Польша и Объединенные Арабские Эмираты, в основном из-за усиленной деятельности кибербанд и государственно поддерживаемых APT [4].
- **APT (Advanced Persistent Threats).** Сложные и долгосрочные атаки, организованные государственными акторами или организованными группами, нацеленные на критическую инфраструктуру и чувствительные данные. Эти атаки трудно обнаружить и могут пройти месяцы или даже годы до их обнаружения.



Источник: Bitdenender [5], Угрозы кибербезопасности. Карта в реальном времени

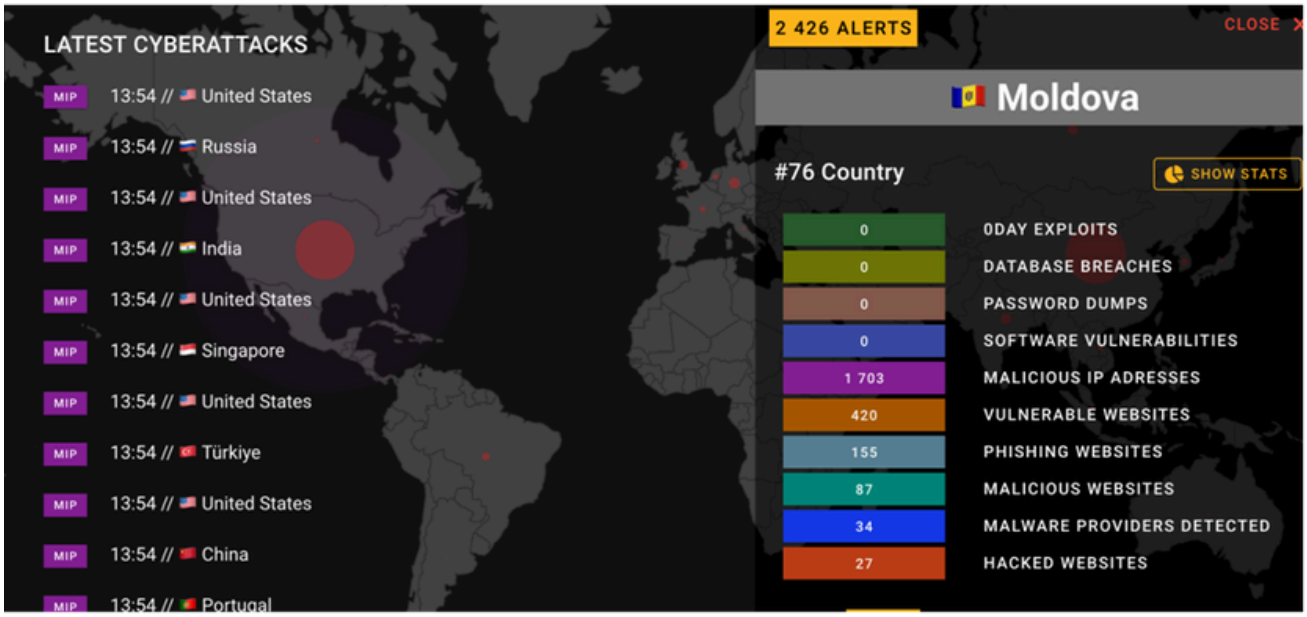
---

[1] COFENSE / PhishMe - Human Phishing Defense Solution. Protectie anti-phishing prin educarea utilizatorului.
https://www.netsafe.ro/phishme-solutie-antiphishing/
[2] 2023 Official Cybercrime Report
https://www.esentire.com/resources/library/2023-official-cybercrime-report
[3] A Retrospective on DDoS Trends in 2023 and Actionable Strategies for 2024
https://www.akamai.com/blog/security/a-retrospective-on-ddos-trends-in-2023 5]
[4] A Retrospective on DDoS Trends in 2023 and Actionable Strategies for 2024
https://www.akamai.com/blog/security/a-retrospective-on-ddos-trends-in-2023
[5] Bitdefender. https://threatmap.bitdefender.com/

Быстрое развития технологий принесло значительные выгоды, но также вызвало вызовы в области кибербезопасности. Новые технологии, такие как Интернет вещей (IoT) [6], искусственный интеллект (AI [7]) и блокчейн [8], открыли новые возможности для инноваций, но также создали новые векторы атак и уязвимости. Важно, чтобы технологическое развитие сопровождалось мощными мерами безопасности для обеспечения защиты от киберугроз.

Большое количество кибератак, которые происходят параллельно и координируются государственными и негосударственными акторами, представляют собой значительные вызовы для глобальной безопасности. Эти атаки часто хорошо финансируются и выполняются с высокой точностью, имея различные цели, от экономического и военного шпионажа до саботажа и нарушения критических систем.

1. Государственные акторы - государства используют кибератаки как инструменты гибридной войны и шпионажа против других государств для получения стратегической информации или нарушения критической инфраструктуры. Один из известных примеров - атака на украинскую энергосеть в 2015 году, приписываемая группе APT Sandworm [9], связываемой с российским правительством. Эта группа значительно усилила свои кибероперации на фоне конфликта в Украине. В действительности, они представляют собой стратегический микс шпионажа, саботажа и дезинформации для подрыва противников. Кроме того, непосредственная угроза, представленная APT 44, подчеркивает критическое вызов в глобальной кибербезопасности и стабильности международных отношений [10].
2. Негосударственные акторы - хакерские группы и киберпреступные организации используют кибератаки для финансовой выгоды или продвижения политических агенд. Только в США, согласно Центру жалоб на интернет-преступления ФБР (IC3), за 2023 [11] год был зафиксирован рекордный уровень жалоб от американской общественности: 880,418 жалоб с потенциальными потерями, превышающими 12,5 миллиарда долларов США, что составляет почти 10% увеличение жалоб и рост на 22% убытков по сравнению с 2022 годом.



Источник: Киберкарта, HTTPCS [12], анализ Республики Молдова

Согласно Глобальному индексу кибербезопасности (GCI), Республика Молдова занимает 63 место. GCI оценивает уровень развития каждой страны на основе её юридических, технических и организационных мер в области кибербезопасности, а также развития её способностей и сотрудничества в этой сфере. Хотя технические меры кибербезопасности Молдовы оцениваются

---

[6] Интернет вещей — это сеть электронных устройств (также называемых «вещами»), содержащих датчики, программное обеспечение и другие технологии, которые подключены к Интернету для обмена данными и взаимодействия с другими устройствами и людьми (также называемыми «пользователями»).https://courses.minnalearn.com/ro/courses/emerging-technologies/the-internet-of-things/an-introduction-to-the-internet-of-things/

[7] Inteligența artificială. https://pisa.md/wp-content/uploads/2023/07/inteligenta-artificiala.jpg

[8] Blockchain este un registru partajat, imuabil, care facilitează procesul de înregistrare a tranzacțiilor și de urmărire a activelor într-o rețea de afaceri https://www.ibm.com/topics/blockchain

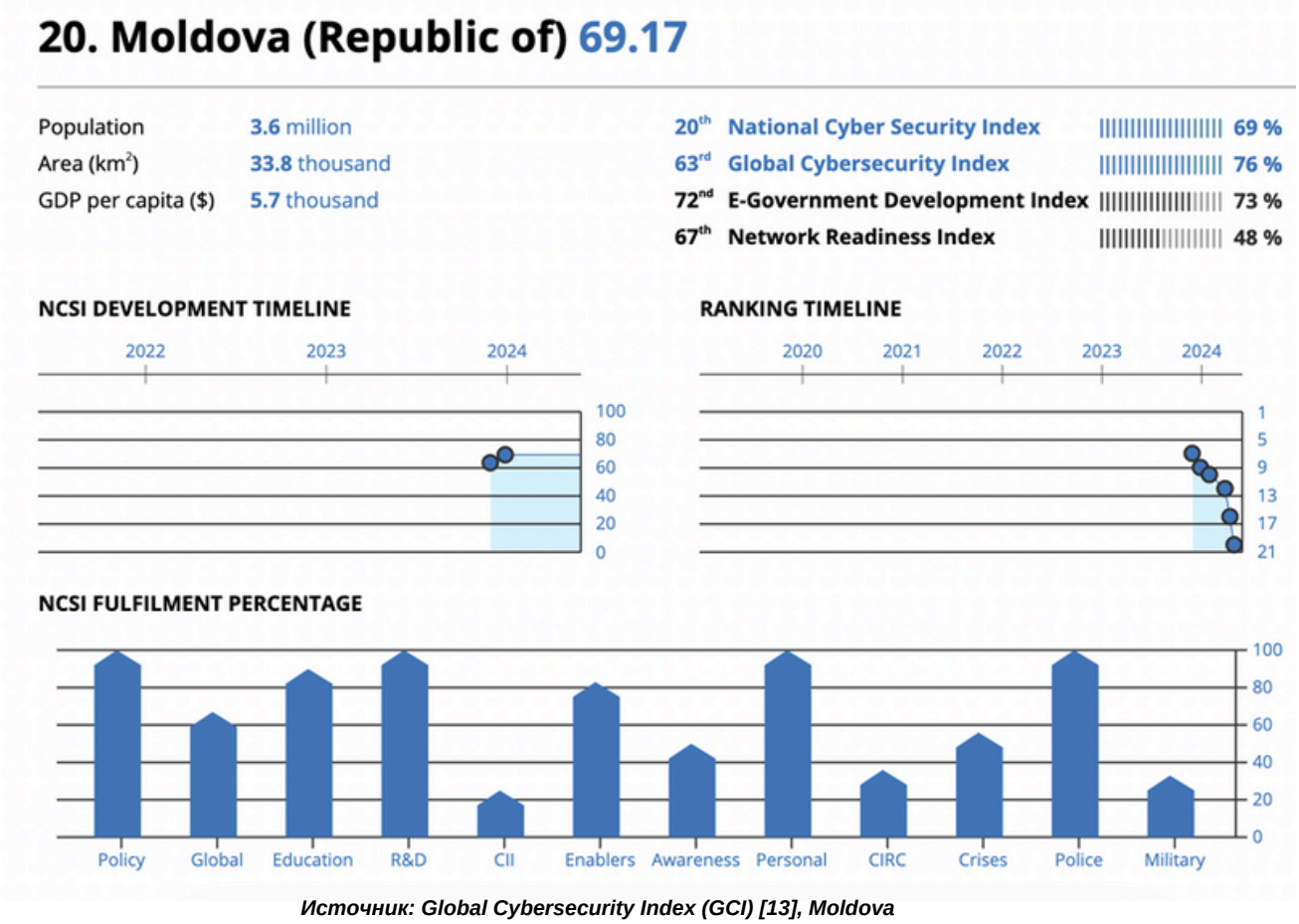
[9] Sandworm Cyberattackers Down Ukrainian Power Grid During Missile Strikes.
https://www.darkreading.com/ics-ot-security/sandworm-cyberattackers-ukrainian-power-grid-missile-strikes

[10] The APT44 Sandworm: A Threat Assessment. https://greydynamics.com/the-apt44-sandworm-a-threat-assessment/

[11] Internet Crime report 2023. https://www.ic3.gov/media/pdf/annualreport/2023_ic3report.pdf

[12] https://map.httpcs.com/country/MD

как «относительно сильные», необходимо улучшить её организацию и развитие способностей. Другие рекомендации от GCI включают разработку стратегии по защите критической инфраструктуры и систематическое внедрение систем управления информационной безопасностью, что потребует увеличения числа министерств, сертифицированных по стандарту ISO 27001.



Источник: Global Cybersecurity Index (GCI) [13], Moldova

Исходя из отчета USAID и данных, предоставленных CERT-GOV-MD (Командой реагирования на компьютерные чрезвычайные ситуации правительства Молдовы), количество кибератак значительно возросло в последние годы [14].
Типология атак:

- **Phishing**: Мошеннические электронные письма, направленные на получение чувствительной информации от пользователей. В 2023 году был зафиксирован рост атак phishing на 45% по сравнению с предыдущим годом.
- **Ransomware**: Вредоносное программное обеспечение, блокирующее доступ к данным до выплаты выкупа. Число случаев ransomware выросло на 50% за последние два года, затрагивая как государственные учреждения, так и частные компании.
- **DDoS (Distributed Denial of Service)**: Атаки, целью которых является перегрузка серверов трафиком для их недоступности. Атаки DDoS усилились, с числом инцидентов, составившим 250 только за первый квартал 2023 года.
- **APT (Advanced Persistent Threats)**: Хорошо финансируемые и оркестрированные атаки, обычно проводимые государствами или организованными группами. APT сложно обнаружить и могут нанести значительный ущерб критической инфраструктуре.

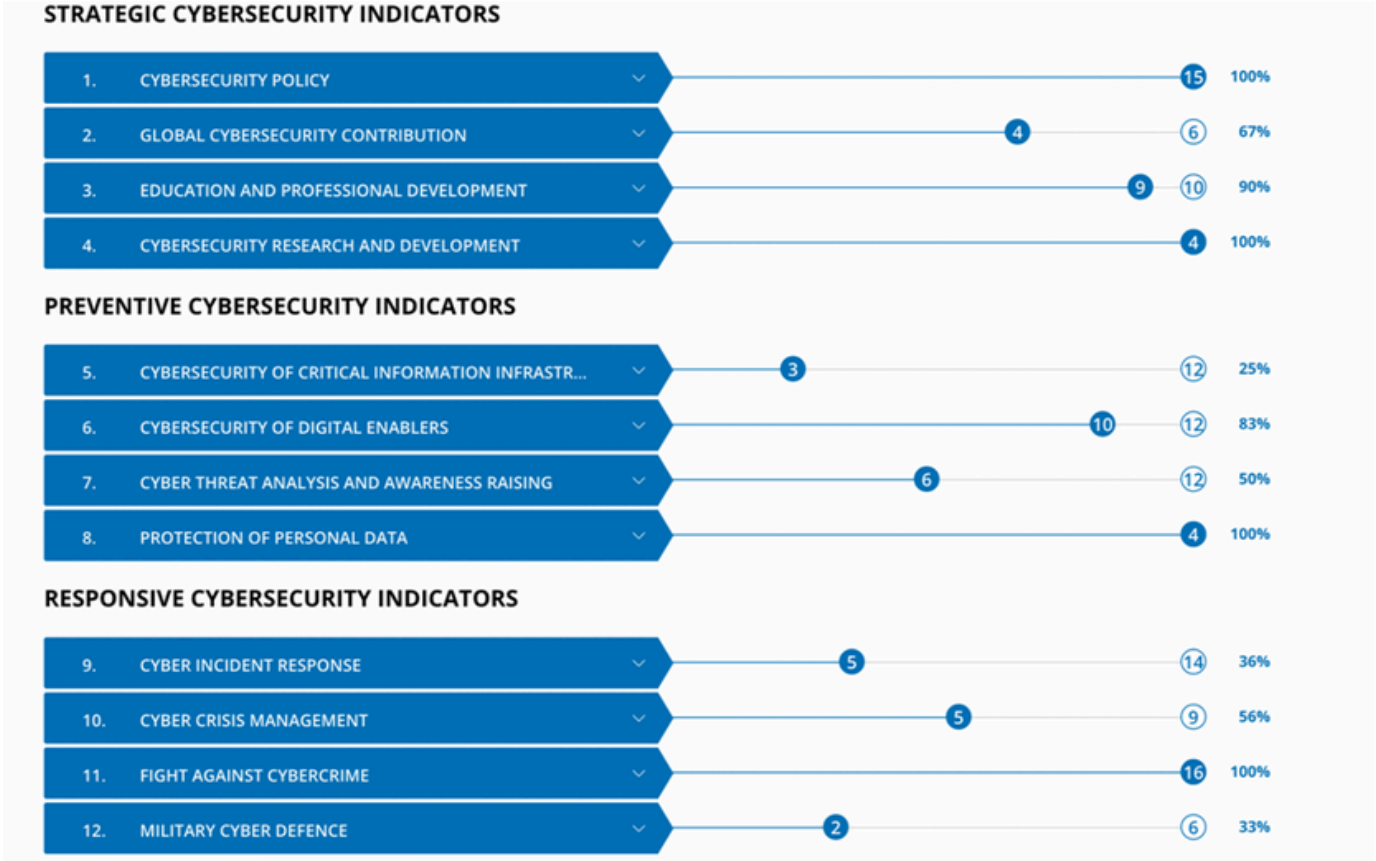
Релевантная статистика:

- В 2023 году было зафиксировано более 1,000 серьезных киберинцидентов.
- Рост атак phishing на 30% по сравнению с предыдущим годом.

Внедрение и капацитет кибербезопасности не успевают за развитием политики. Правительство постоянно вводит меры регулирования и политики в области кибербезопасности в рамках усилий по согласованию с протоколами ЕС. Однако при реализации требуется дополнительная поддержка, что объясняется частично фрагментированным кибербезопасным экосистемой,

[13] Global Cybersecurity Index.
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
[14] Evaluarea ecosistemului digital la nivel de țară digital ecosystem country assessment (DECA)
https://www.usaid.gov/sites/default/files/2023-01/Moldova%20DECA%20%28Romanian%29.pdf

недостаточной доступностью специалистов в области кибербезопасности и недостатками в технических возможностях правительства. Выделение финансовых и человеческих ресурсов также недостаточно для растущих и изменяющихся потребностей в кибербезопасности. Правительственная команда по компьютерным чрезвычайным ситуациям (CERT) является небольшой, но все еще служит связующим звеном для всех коммуникаций и отчетности по кибербезопасности. Другие правительственные органы, такие как Генеральная прокуратура и Министерство внутренних дел, также занимаются вопросами кибербезопасности [15].



Источник: NCSI, Moldova, Raport decembrie 2023, https://ncsi.ega.ee/country/md/?pdfReport=1

Ответ на современные киберугрозы в любой стране требует согласованных усилий множества институций. Координация включает назначение четких ролей и обязанностей соответствующим учреждениям и их способность их выполнять. Национальные команды по реагированию на компьютерные чрезвычайные ситуации или инциденты безопасности (CERT/CSIRT) действуют как ключевые точки контакта для всех заинтересованных сторон (государственные, частный и общественный сектор). Они обычно отвечают за обмен информацией и координирование правительственных ответов на киберинциденты. В феврале 2024 года Республика Молдова запустила Национальное агентство кибербезопасности, которое направлено на защиту критической инфраструктуры государства и общества от кибератак, обеспечивая высокий уровень безопасности для информационных технологий государственных и частных учреждений [16]. Также институциональная структура обеспечения кибербезопасности разделена между следующими учреждениями: Министерство экономики, Служба информационных технологий и кибербезопасности (STISC), Команда по реагированию на компьютерные чрезвычайные ситуации в составе STISC (CERT-GOV-MD), Агентство по электронному управлению, Министерство обороны, Министерство внутренних дел, Служба информации и безопасности, Генеральная прокуратура, Администрация Президента и Комиссия по национальной безопасности, обороне и правопорядку Парламента Республики Молдова.

Из DDoS-атак и социальной инженерии являются наиболее часто встречающимися типами киберугроз. Служба информации и безопасности Республики Молдова описывает четыре основных типа киберугроз: DDoS-атаки, фишинг через электронные письма от государственных

[15] Evaluarea ecosistemului digital la nivel de țară digital ecosystem country assessment (DECA) https://www.usaid.gov/sites/default/files/2023-01/Moldova%20DECA%20%28Romanian%29.pdf
[16] Moldova launches new national cybersecurity bodies during first Cybersecurity Forum. https://eufordigital.eu/moldova-launches-new-national-cybersecurity-bodies-during-first-cybersecurity-forum/

учреждений, атаки методом перебора паролей для получения доступа к государственным информационным системам и взлом официальных веб-сайтов. CERT-GOV-MD подтвердил, что наиболее распространенными киберугрозами в Молдове являются DDoS-атаки, мошеннические платежи (связанные с цифровыми услугами), социальная инженерия (фишинг, обман, фейковые новости, дезинформация) и кражи данных.

Рекомендации

Киберустойчивость представляет собой способность быстро сопротивляться и восстанавливаться после кибератак. В Республике Молдова развитие этой устойчивости необходимо для защиты критической инфраструктуры, такой как энергетические сети, финансовые системы и коммуникации. Многие из этих инфраструктур используют устаревшие технологии, уязвимые для атак, требующие внедрения строгих протоколов безопасности и эффективных систем резервного копирования. Постоянная проверка безопасности и принятие международных лучших практик являются ключевыми для укрепления безопасности этих инфраструктур.

Быстрый и эффективный отклик на кибератаки необходим для минимизации их влияния путем укрепления национальных команд CERT, оснащения их последними ресурсами и технологиями, а также проведения регулярных учений и симуляций. Международное сотрудничество с организациями, такими как ENISA и НАТО, обеспечивает доступ к важной информации и ресурсам для предотвращения и борьбы с кибератаками, а обмен информацией с другими государствами помогает решать общие угрозы.

Образование и осведомленность общественности играют важную роль в защите граждан от кибератак. Проведение национальных кампаний осведомленности, создание доступных руководств и ресурсов для граждан и малых предприятий, а также включение кибербезопасности в учебные программы школ и университетов способствуют повышению уровня защиты. Программы непрерывного обучения для IT-специалистов и широкой общественности, вложения в стартапы и сотрудничество с частным сектором являются неотъемлемыми составляющими развития кибербезопасного экосистемы в Молдове.