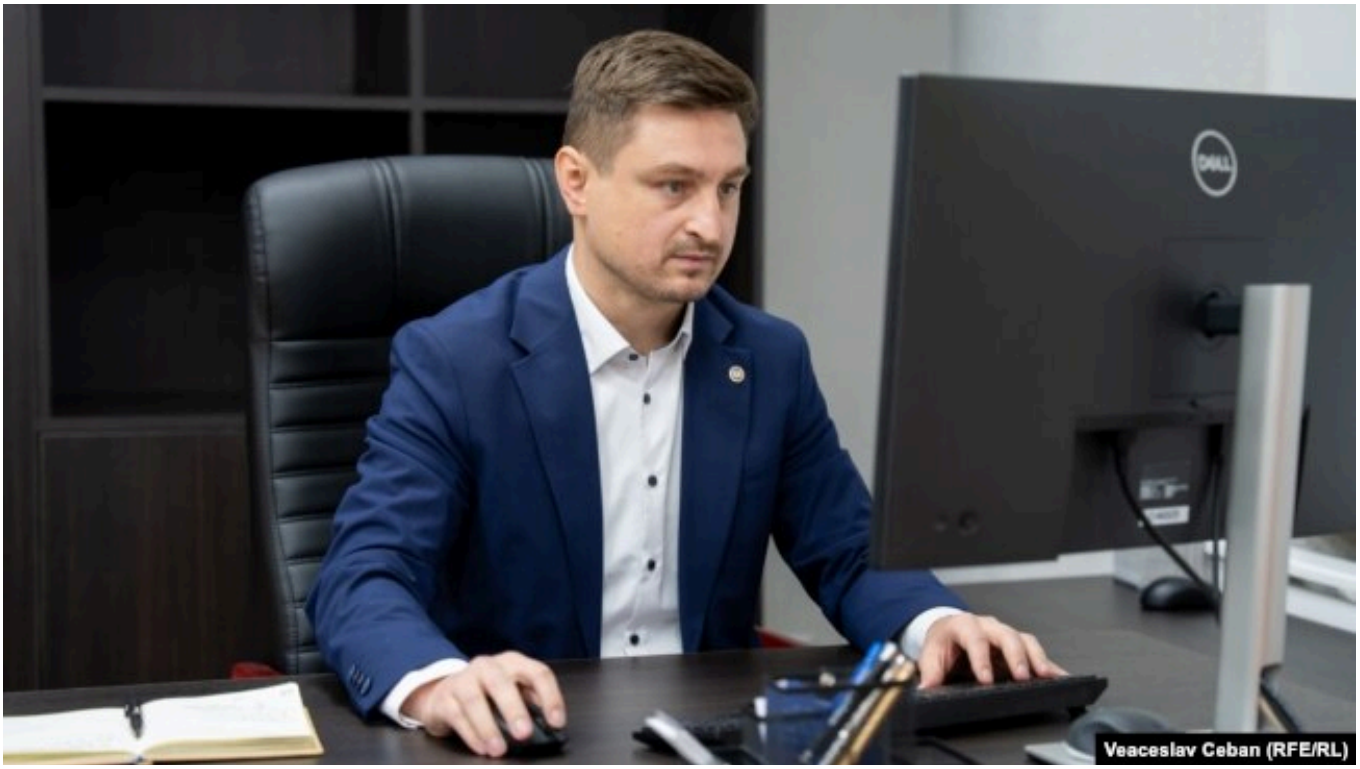
View the original article

МОЛДОВА

Глава Агентства кибербезопасности Молдовы о взломе госуслуг и хищении данных трети жителей: "Возможности AI будут порождать киберинциденты"

Эуген Урушук

3 ноября 2026 года 06:00 мск



Михай Лупашку, директор Агентства кибербезопасности Республики Молдова

В конце октября в Молдове произошла крупнейшая кибератака в цифровой истории страны: был взломан сервис госуслуг EVO (evo.gov.md) и украдены цифровые данные 750 тыс. человек, то есть примерно трети населения страны. Речь идет об именах, идентификационных номерах граждан, сведениях о членах их семей, данных водительских удостоверений, пенсиях и финансовых данных, включая налоговые задолженности. Чтобы остановить кибератаку, властям Молдовы 23 октября пришлось

временно отключить 82 государственных сервиса и более 30 информационных систем. Полностью восстановить работу удалось только утром 27 октября.

В числе пострадавших — топ-чиновники и государственные деятели. По иронии судьбы, одним из них был глава Агентства кибербезопасности Молдовы **Михай Лупашку.**

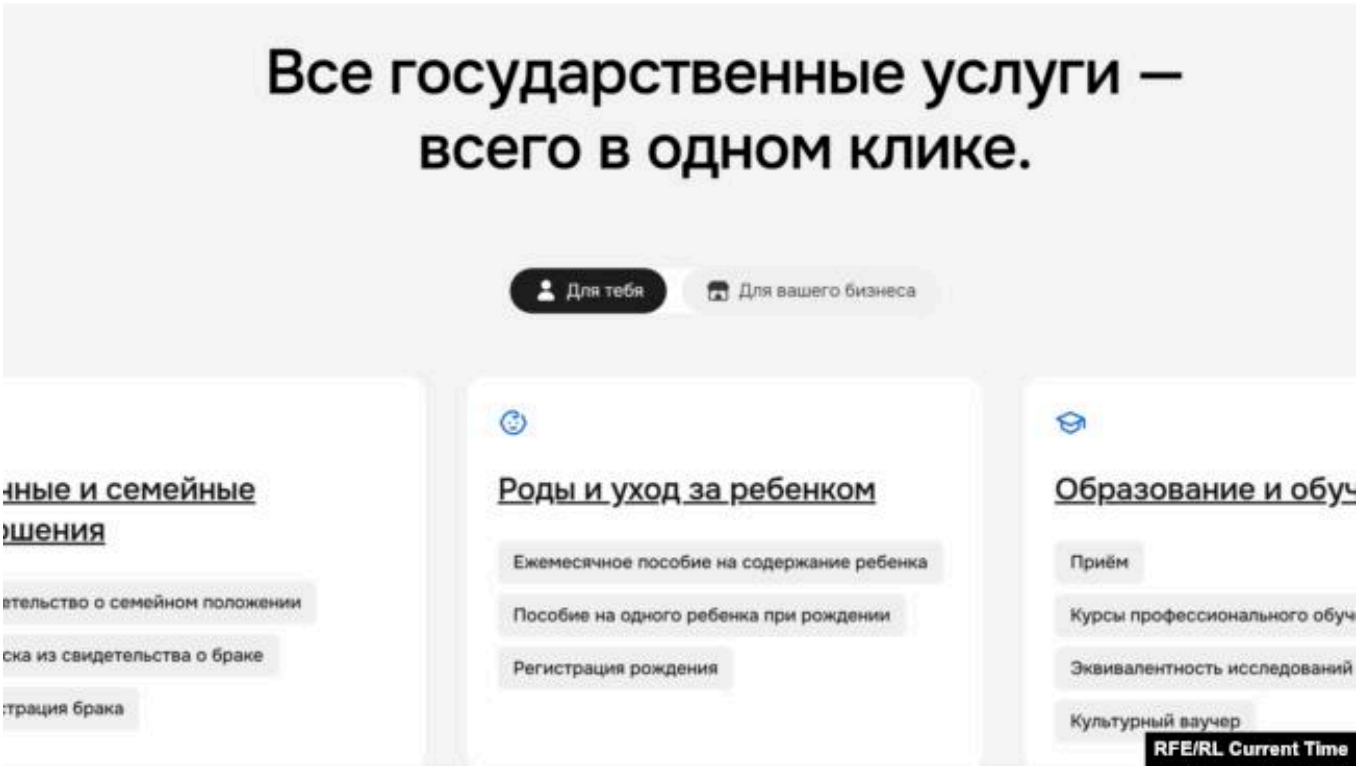
В интервью молдавской службе Радио Свобода Лупашку рассказал, как произошла крупнейшая кибератака в Молдове. Он считает взлом не случайностью, а "тщательно спланированной акцией", организованной "хорошо подготовленными" хакерами: по его словам, они обнаружили уязвимости в государственной цифровой системе с помощью искусственного интеллекта.

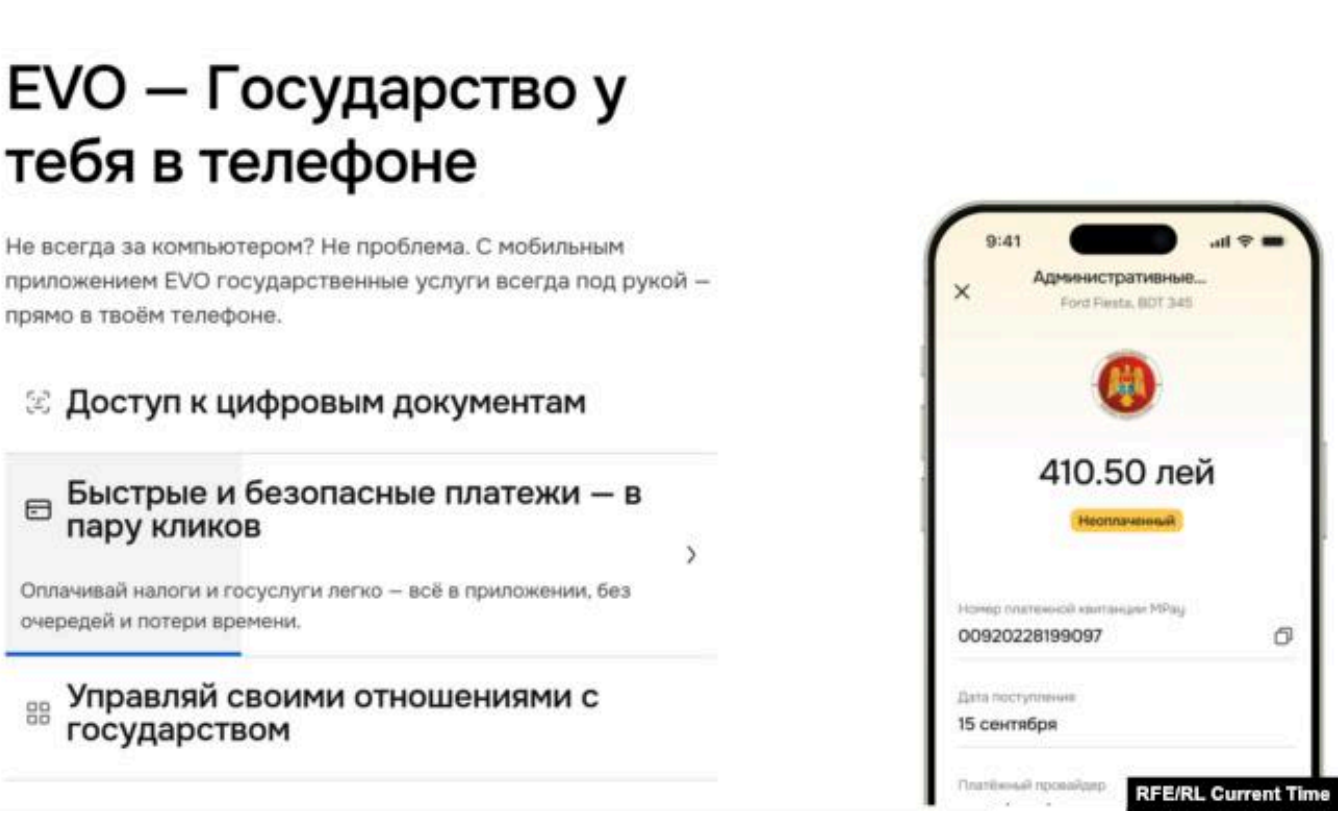
*****

"Кибератака проводилась преимущественно вечером и ночью"

— Власти Молдовы объявили, что объектом кибератак на цифровые государственные сервисы были около миллиона персональных числовых идентификаторов (IDNP), и что в результате были похищены данные примерно 750 тыс. граждан Молдовы. Вы тоже оказались в числе жертв этой атаки?

— Да, я подтверждаю, что вхожу в число 750 тыс. граждан, чьи персональные данные были доступны третьим лицам.





— Какие протоколы действуют в подобных ситуациях? Вы, как глава Агентства кибербезопасности, когда узнали об этой атаке и каковы были ваши первые действия?

— Агентство кибербезопасности было уведомлено о кибер-инциденте на позапрошлой неделе. Было установлено, что в период с 19 по 23 октября были использованы несколько уязвимостей в информационных системах, управляемых агентством AGE (Агентство электронного управления Молдовы, E-Governance Agency, Agenția de Guvernare Electronică, разработчик EVO).

23 октября инцидент был подтвержден, и было принято беспрецедентное решение о приостановке доступа к некоторым госсервисам — чтобы ограничить последствия и позволить провести более детальный анализ произошедшего и способов исправления ситуации.

— Кто проводит проверку ситуации?

— Каждое учреждение работает в своей области компетенции, участвуют коллеги из всех соответствующих учреждений – из Центра расследования киберпреступлений, Агентства по кибербезопасности, Службы информационных технологий и кибербезопасности, Агентства электронного управления... Все работают над своими компонентами, чтобы дать наиболее ясные ответы и прояснить ситуацию.

— Кто из руководства страны был проинформирован первым?

— Существует протокол связи со всеми учреждениями, участвующими в этом процессе. Коллеги из AGE уведомили всех заинтересованных лиц, как только обнаружили кибератаку. Нас также проинформировали в тот момент, как и группу реагирования на инцидент, которая отправилась оказывать помощь и расследовать обстоятельства нападения.

— Эти уведомления были сделаны днем или ночью? Как это произошло?

— Мы наблюдали, что кибератака проводилась определенным способом, преимущественно вечером и ночью — поскольку обнаружить активность в часы, когда нет наблюдения, сложнее.

СМОТРИТЕ ТАКЖЕ:
Во Франции хакеры взломали холодильники в сотнях супермаркетов: продукты нагрели до 50 грудусов

Мы назвали атаку "инцидентом", но на самом деле это была серия действий, волн и попыток кибератак, которые были очень изощренными и были направлены на целый ряд сервисов. Речь шла не об одном сервисе или одной информационной системе. Мы говорим о ситуации, когда очень хорошо подготовленный киберпреступник действовал с совершенно ясной целью — скомпрометировать информационные системы и похитить данные.

— Возможно ли, что в ходе этой волны атак были также получены личные данные молдавского руководства – президента, спикера парламента или премьер-министра?

— Я не могу подтвердить эту информацию. Но каждый гражданин, или, по крайней мере, те, кто используют приложение EVO, могут проверить историю доступа к своим персональным данным в профиле пользователя. Коллеги из AGE работают над механизмом, с помощью которого мы проинформируем каждого гражданина из 750 тыс. пострадавших о данных, к которым был получен доступ в его конкретном случае.

"В кибератаке были задействованы 700 различных IP-адресов"

— То, что произошло, является крупнейшей кибератакой в истории цифровой инфраструктуры Республики Молдова?

— Безусловно да, можно сказать, что это самая крупная кибератака из всех зарегистрированных на данный момент.

В период выборов, в 2025 и 2024 годах, у нас были волны и крупные кибератаки, но по масштабу последствий эта — самая масштабная. Сейчас технические специалисты работают над устранением ее последствий и предотвращением других негативных последствий. Окончательный вывод будет сделан после завершения инцидента, изоляции инфраструктуры и составления итогового отчета.

СМОТРИТЕ ТАКЖЕ:

За взломом крупнейшей в мире криптовалютной биржи Binance могут стоять хакеры из Северной Кореи – TRM Labs и Pangolin Intelligence

— Какие именно уязвимости позволили хакерам вызвать масштабный цифровой кризис в Республике Молдова?

— В приложениях было обнаружено несколько уязвимостей. Хочу заметить, что в цифровом мире любое приложение может в какой-то момент стать уязвимым. Сейчас задействованы возможности сервисов искусственного интеллекта (ИИ), в том числе те, которые позволяют выявлять уязвимости в гораздо больших масштабах и гораздо быстрее, чем это могут сделать люди.

Сейчас мы находимся в переходном периоде, и изменения затрагивают не только Молдову. Это не умаляет серьезности инцидента, о котором мы сейчас говорим, но мы должны понимать, что возможности искусственного интеллекта будут продолжать порождать кибер-инциденты в ближайшие несколько лет.

Более эффективный механизм защиты отныне должен включать переписывание и перепроектирование некоторых цифровых сервисов, в том числе с использованием инструментов искусственного интеллекта. Мы должны признать, что многие из сервисов, используемые [в Молдове], были написаны и разработаны человеческим интеллектом, то есть людьми. Теперь, с помощью инструментов искусственного интеллекта, можно обнаружить уязвимости, которые человек не может выявить.

— Сколько кибератак, крупных и мелких, произошло в Молдове в этом году?

— У меня нет под рукой статистики, но могу сказать, что за год в Агентство кибербезопасности поступили сообщения о десятках атак, в которых потребовалось вмешательство группы реагирования на инциденты.

Мы должны понимать, что кибератаки никогда не прекращаются, это непрерывное явление. Это реальность, в которой мы живем. Сейчас наши приоритеты — устранение последствий, обеспечение безопасности и запуск сервисов безопасным способом, позволяющим гражданам получать к ним доступ.

— У вас есть хотя бы смутное представление о происхождении хакеров, организовавших последнюю атаку? Это атака, скоординированная другим государством, или киберпреступлении со стороны частных лиц?

— На данном этапе преждевременно делать какие-либо выводы. Мы собираем все технические данные, связанные с этой атакой. Мы уже сообщили о 700 различных IP-адресах, которые были идентифицированы или которые были задействованы в этой кибератаке.

Из-за особенностей функционирования интернета мы не можем с уверенностью назвать конкретного злоумышленника, стоящего за этим, но я почти уверен, что мы узнаем больше об организаторах.

Могу лишь отметить, анализируя сложность инцидента, что это не случайная атака, а сложная и хорошо подготовленная. Соответственно, это кое-что говорит нам о потенциальных участниках, которые могут за ней стоять. Речь идет не об одном человеке, который случайно попытался скомпрометировать сервис. У людей, стоящих за этим, есть технические возможности и инфраструктура, позволяющие им организовывать и координировать подобные атаки.

СМОТРИТЕ ТАКЖЕ:

Хакеры из группировки ShinyHunters украли медицинские данные агентов ФБР

"Люди получили заверения, что их данные не будут использованы для получения кредитов"

— Я один из тысяч пользователей приложения EVO — этого цифрового кошелька для документов и единой точки доступа к государственным услугам. И я узнал, что мои данные также были украдены. Какие гарантии безопасности вы можете предложить пользователям приложения в данный момент?

— На данный момент мы точно знаем, что никаких изменений в данные граждан Молдовы внесено не было, они были только извлечены. Это тоже серьезно, это может привести к использованию данных для попыток телефонного мошенничества, интернет-мошенничества, выдачи себя за другое лицо или попыток выдачи себя за другое лицо. По сути, это не является новым явлением. Но мы должны признать, что с учетом объема извлеченных данных создается гораздо больший потенциал для мошенничества.

— Многие граждане обеспокоены: существует ли риск того, что украденная информация будет использована злоумышленниками для получения банковских или небанковских кредитов с помощью поддельных документов?

— Лучше задать этот вопрос коллегам из банковского сектора или Национального банка Молдовы (НБМ). Но на данный момент, исходя из имеющейся у нас информации, риск использования этих данных для оформления кредитов в банках или других кредитных учреждениях исключен. Я не уполномочен говорить от имени НБМ, но граждане получили заверения, что соответствующие данные не будут использованы для получения кредитов.

СМОТРИТЕ ТАКЖЕ:

Microsoft сообщила о масштабной кампании российских хакеров по взлому сетей Wi-Fi в отелях по всему миру

— В результате атаки в Молдове была приостановлена работа ряда государственных онлайн-сервисов. Какая часть цифровой инфраструктуры правительства пострадала и какая часть уже восстановлена?

— Согласно последним данным, представленным AGE, необходимо было восстановить около 70 цифровых сервисов. AGE предполагает, что все затронутые сервисы будут восстановлены в течение этой недели.

— В какой степени, по вашему мнению, этот цифровой кризис подорвал доверие граждан к процессу цифровизации и к государственным структурам в Молдове?

— Безусловно, это влияет на восприятие и на безопасность, которая в настоящее время находится под вопросом. Для соответствующих учреждений будет очень важно восстановить доверие населения и быть прозрачными в информировании о причинах инцидентов и мерах, принятых для предотвращения подобных инцидентов в будущем. Безусловно, необходимо извлечь уроки и внести коррективы, чтобы избежать подобных уязвимостей в будущем.

Читай нас в Телеграме

ПОДПИСАТЬСЯ

МАТЕРИАЛ ИЗ РАЗДЕЛОВ:

Видео и статьи | Интервью | Молдова

© Настоящее Время. Все права защищены