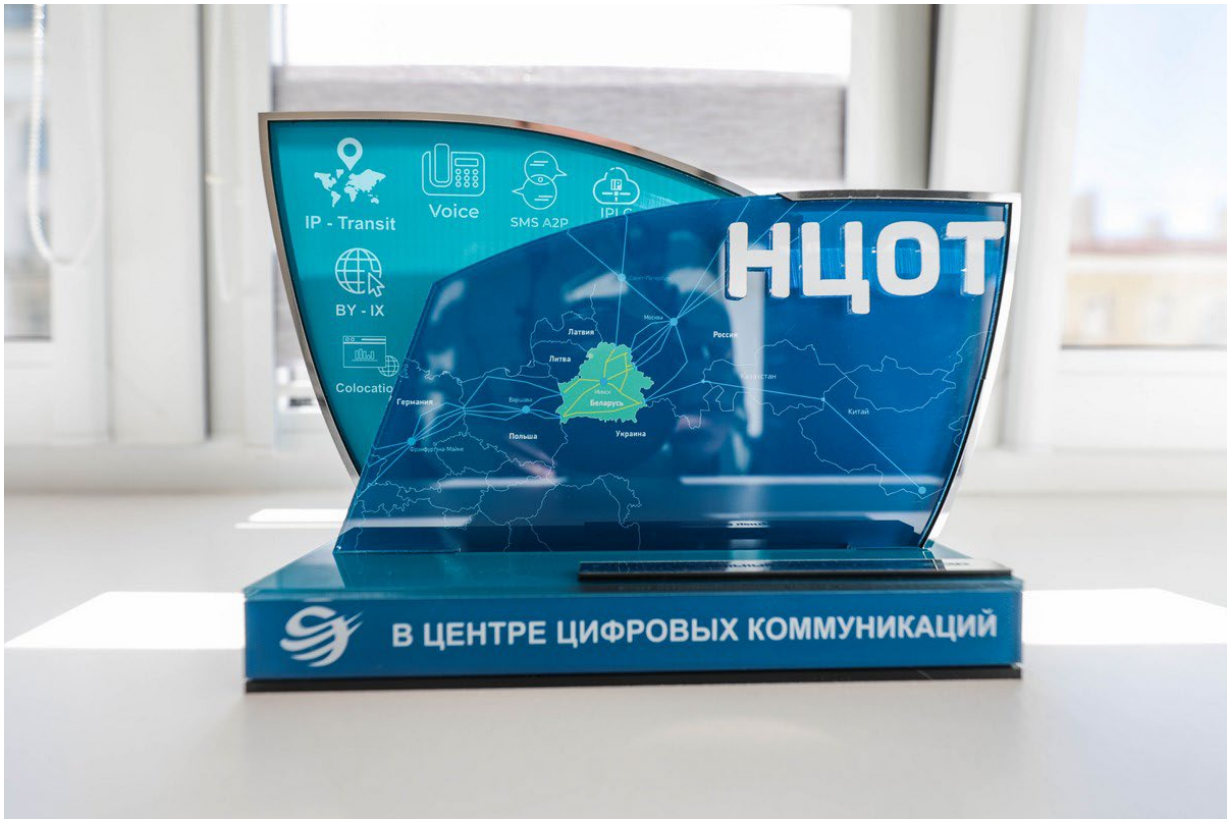
Опубликовано: 7 мая 09:30

ИСТОЧНИК: СБ БЕЛАРУСЬ СЕГОДНЯ

Наш киберответ! РУП «Национальный центр обмена трафиком»

По данным Национального центра обмена трафиком, кибератаки на предприятия национальной экономики стали более организованными и системными



Поскольку жизнь и работа миллионов людей становятся более зависимыми от интернет-технологий, вопросы кибербезопасности набирают критическую актуальность. Без должной защиты все уязвимее сохранность личных данных, значительной угрозе подвергается деятельность компаний и предприятий. В мире возрастает количество хакерских атак на госучреждения, крупные промышленные корпорации, бизнес, сферы финансов, здравоохранения и телекоммуникаций. А уровень подготовки взломщиков растет. В таких условиях опасна социальная пассивность — необходимы адекватные ответные меры.
Какие действия предприняты у нас в стране, чтобы противодействовать неправомерному доступу к охраняемой законом информации?

Должная бдительность

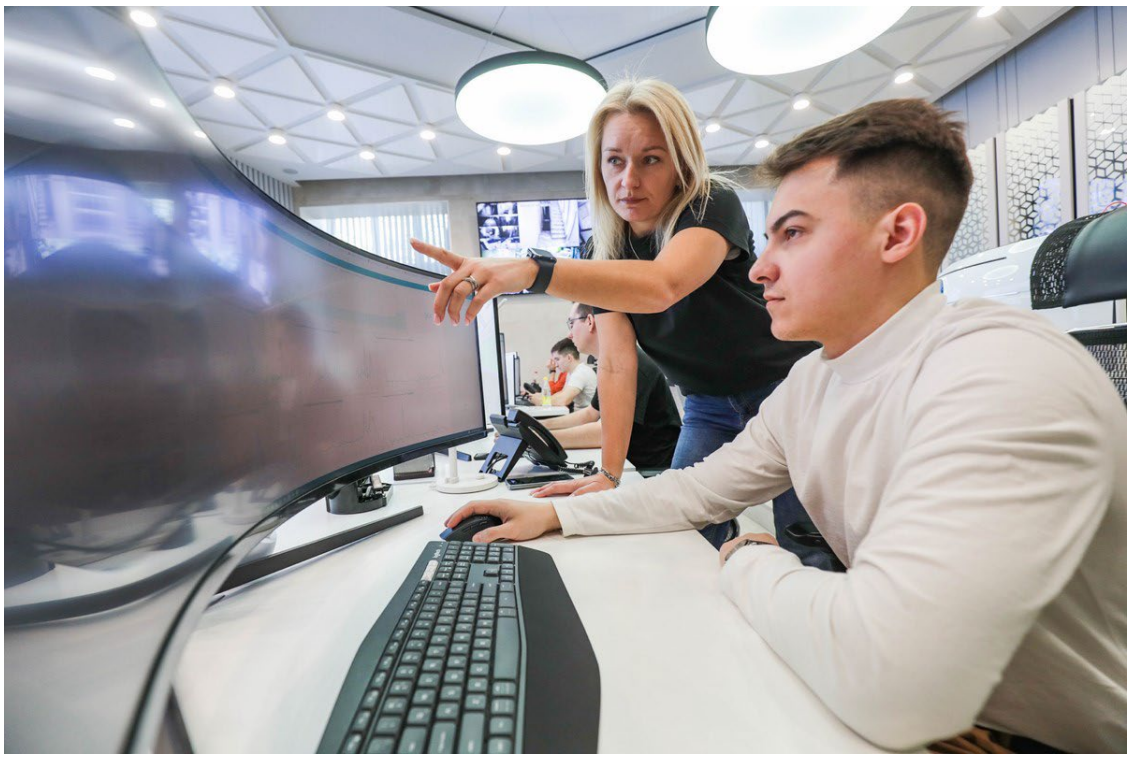
— Как и зарубежные коллеги, мы отмечаем рост продолжительности и интенсивности кибернападений. Информационные атаки стали более организованными и системными. Но далеко не все компании всерьез воспринимают существующие угрозы и в полной мере выстраивают систему защиты информации, — поясняет суть проблемы директор РУП «Национальный центр обмена трафиком» Алексей Цымбалов. *— А ведь действенный взлом сети, например оператора электросвязи, может критически отразиться на качестве сервиса для огромного количества клиентов. Уже в 2024 году кибератаки на крупных операторов привели не только к утечке данных абонентов, но и к недоступности интернета и сотовой связи. Пагубный опыт показал: для проведения информационной атаки необходимо несколько дней, на устранение ее последствий — недели.*

Алексей Цымбалов.

За киберзащитой стоит обращаться не по факту, а заблаговременно, на постоянной основе, тогда компания защитит себя от убытков из-за простаивания бизнеса, которые могут исчисляться миллионами рублей.

Основная цель хакеров и их группировок — вымогательство, обычно под предлогом уничтожения данных либо их опубликования в открытом доступе. И это не только подрывает безопасность компаний, приводит к финансовым потерям, но и серьезно угрожает ее репутации. Часто злоумышленники используют вирусы, которые при заражении одного компьютера способны распространяться по сети и шифровать ценную информацию практически без возможности ее восстановления.

Еще одна цель — перехват управления веб-сайтом предприятия для распространения ложных сведений. Иногда взломанная страница используется для проведения цепочки атак на «более крупную добычу», как промежуточная точка входа, чтобы скрыть следы неправомерных действий.

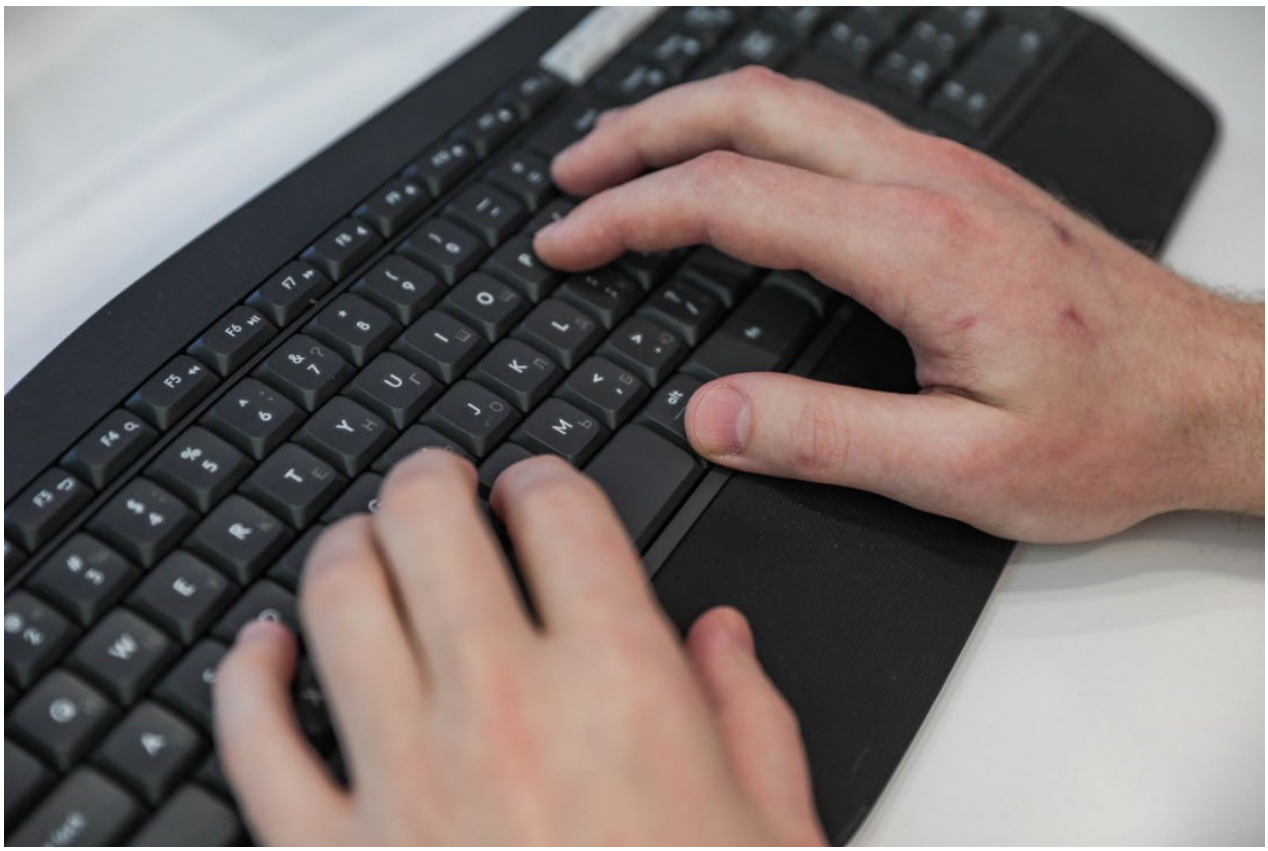


Скрытые утечки

Специалисты предупреждают: важно уметь распознать подозрительные сообщения в мессенджерах и электронных письмах, поскольку одним из частых инструментов кибератак стал фишинг. При помощи поддельных копий сайтов или аккаунтов жертву обманом вынуждают к предоставлению ценной информации.

— Нередко совершаются атаки, связанные с отказом в обслуживании (DDoS): мошенники пытаются вызвать перегрузку сервиса, отправляя на него аномально большое количество запросов. Цель очевидна — сделать атакуемую веб-страницу недоступной для реальных пользователей, — обращает внимание Алексей Александрович. *— НЦОТ ежегодно фиксирует в инфраструктуре — собственной и своих клиентов — более 35 тысяч DDoS-атак разной степени интенсивности. И мы защищаем клиентов от такого вмешательства.*

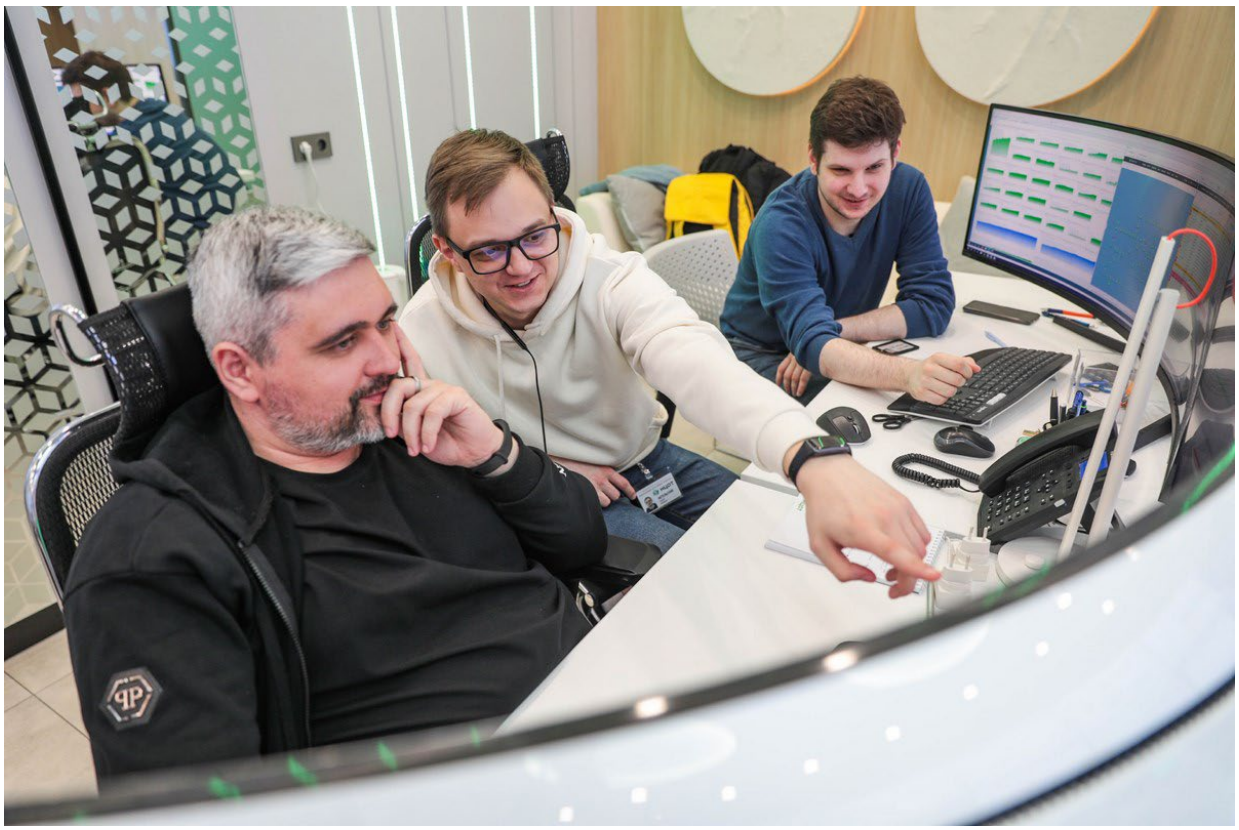
Прогноз по количеству кибератак, к сожалению, неблагоприятен. Их численность будет расти — вопрос лишь в том, какими темпами. Такого рода агрессивные меры способны поражать большое количество целей. Как правило, они вызывают серьезный общественный резонанс. 2022-й и 2023-й в мире называют годами утечки информации. 2024-й, вероятно, назовут годом скрытых утечек из-за того, что хакеры незаметно похищают данные, а затем, спустя время, реализуют негативные сценарии в виде отказа инфраструктуры.



Компаниям необходима своя команда квалифицированных профессионалов в сфере информационной безопасности, которая будет непрерывно отслеживать и реагировать на аномалии в инфраструктуре. На рынке труда на «ибэшников» повышенный спрос. И в условиях, когда высоких компетенций недостаточно, решение — реализация Указа - Президента Республики Беларусь № 40 «О кибербезопасности».

Чтобы обеспечить предприятия необходимыми профессионалами, в 2020 году на базе НЦОТ был создан Международный центр образования ROZUM, где технически подкованные специалисты могут повысить квалификацию в области информационной безопасности. К тому же НЦОТ первым в стране аттестовал свой центр кибербезопасности и начал оказывать услуги для организаций по комплексному подходу к защите своих данных.

Одни из наиболее востребованных услуг центра — проектирование, создание и аттестация систем защиты информации. Следом за ними — круглосуточный мониторинг событий, возможных кибер-инцидентов различного уровня сложности. Такой подход позволяет не дожидаться, когда злоумышленник начнет «ломать» инфосети, а пресечь его действия еще на стадии разведки и анализа.



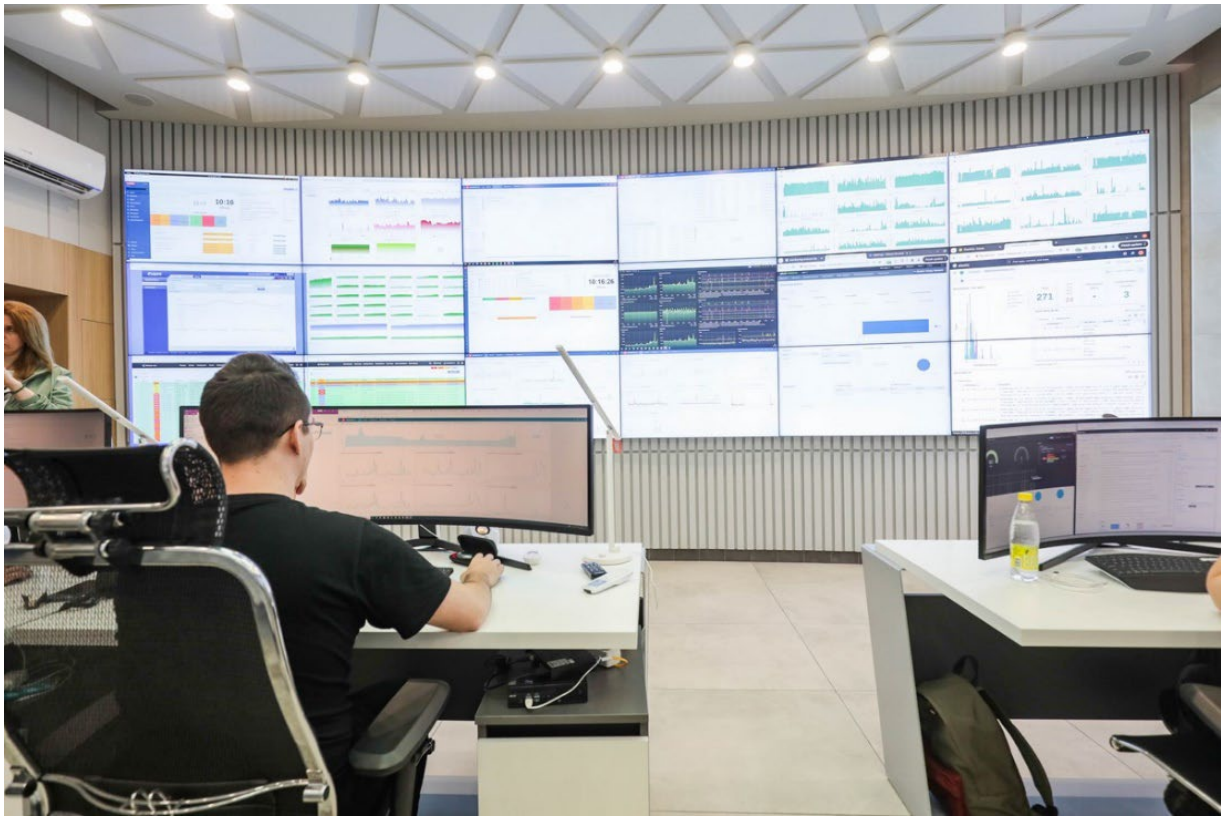
Учения на киберполигоне

— В Международном центре образования ROZUM представлено более 20 программ повышения квалификации по информационной безопасности в целом и кибербезопасности в частности. Приветствуется максимально практико-ориентированный поход. В 2023 году совместно с «Ростелеком-Солар» в ROZUM прошли обучение 95 человек, которые испытали свои силы на нашем киберполигоне, — комментирует заместитель директора Виталий Карбовский. *— Эта площадка — своего рода макет инфраструктуры крупного предприятия: его информационных систем, базы данных, сети, рабочих мест. Здесь происходит отработка поиска уязвимости с использованием различных систем взлома. И поскольку киберпреступники становятся все более изощренными, используют новые «отмычки» для проникновения, модификация — доработка и усложнение полигона — всегда актуальна. Специалистам, которые приходят к нам заниматься, очень важна и интересна такая практика.*

Взаимодействуя с различными предприятиями и крупными холдингами, НЦОТ не раз показывал руководству и IT-отделам слабые места в мерах по защите информации. Очевидный пример — наличие открытых портов, доступных из интернета, через которые можно управлять внутренней инфраструктурой. Вопрос времени, когда злоумышленник проникнет или

скомпрометирует узел через бреши в системе.

Подобное недавно случилось с компанией, обрабатывающей большие объемы информации. Через «пробелы» на веб-сайте параллельно с фишинговой атакой захватили один из серверов внутри организации. Злоумышленник зашифровал все данные систем хранения и удалил доступные резервные копии. Временно бизнес-процессы предприятия были остановлены. Специалисты НЦОТ восстановили ее деятельность, а далее внутреннюю инфраструктуру перестроил и взял на мониторинг центр кибербезопасности. И поскольку компания остается интересной для хакеров, киберцентр фиксирует и пресекает направленные в ее сторону атаки.



АЛЬЯНС ИНТЕРЕСОВ

Среди перспективных задач Национального центра обмена трафиком — вывести белорусских специалистов в сфере кибербезопасности на максимально высокий уровень подготовки не только за счет работы МЦО ROZUM, но и с помощью активного взаимодействия с вузами.

НЦОТ сотрудничает с БГУИР по введению с 2025 года в образовательную программу университета нового предмета — расследование киберинцидентов — при подготовке специалистов факультета

информационной безопасности. Студенты будут обучаться на киберполигоне центра, выполняя практические задачи по противодействию нападениям хакеров.

Алла МАРТИНКЕВИЧ

Фото: Елизавета КОБЕЦКАЯ