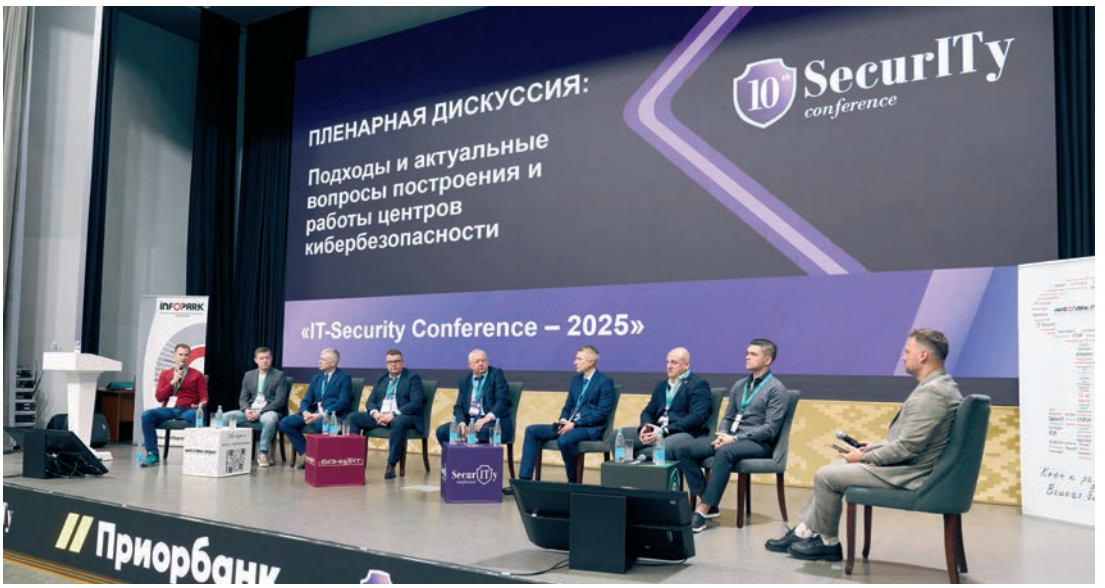

КИБЕРБЕЗОПАСНОСТЬ: О ЧЕМ ГОВОРИТ СООБЩЕСТВО?

Актуальные вопросы в области построения системы кибербезопасности на пленарной дискуссии обсудили руководители восьми центров кибербезопасности Беларуси, а также представитель Оперативно-аналитического центра при Президенте Республики Беларусь как регулятора.

СОЗДАНИЕ ЦЕНТРОВ: ОТ ЗАДАЧ К РЕЗУЛЬТАТАМ

2024 год стал переломным для белорусской системы кибербезопасности. На протяжении года в республике активно создавались центры кибербезопасности, перед которыми стояли масштабные задачи: формирование штатной структуры, закупка оборудования, набор персонала и интеграция объектов инфраструктуры. Как отметил один из участников, «12 месяцев пролетели как 12 недель».

В 2025 году приоритеты сместились на оптимизацию процессов, обучение сотрудников и подключение новых объектов, включая критически важные объекты информатизации.

Обсудили участники дискуссии и технологии, внедряемые для защиты.

OPEN SOURCE VS ПРОПРИЕТАРНЫЕ РЕШЕНИЯ

Сегодня, по словам модератора дискуссии – официального представителя Kaspersky в Беларуси Дмитрия Кудревича, все аттестованные центры кибербезопасности используют проприетарные решения компании Kaspersky. По мнению представителей центров, эти продукты наиболее полно «закрывают» потребности для построения защиты. От внедрения же решений open source большинство останавливает отсутствие технической поддержки и сертификации, а также непредсказуемость обновлений.

При этом опыт использования решений open source в работе отечественных центров кибербезопасности тоже есть: точечные решения используются для автоматизации процессов и тестирования. «Open source – не магия. Если у вас нет экспертизы, лучше полагаться на вендорские решения», – отметил один из участников дискуссии.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ПОМОЩНИК, НО НЕ ЗАМЕНА СПЕЦИАЛИСТАМ

Тему ИИ в построении защиты от внешних угроз эксперты тоже затронули. По словам директора департамента кибербезопасности ОАО «Белагропромбанк» Юрия Карпука, технология применяется в банковском секторе во внедренных антифрод-системах для борьбы с мошенничеством. Но не более. В вопросах кибербезопасности ИИ пока допускает множество ошибок и в качестве замены специалистам первой линии рассматриваться не может.

А вот как инструмент для консультирования использовать ИИ, по мнению экспертов в области кибербезопасности, возможно. Но только при наличии достаточного опыта и знаний у специалистов, чтобы при необходимости распознать ложную информацию. Модератор дискуссии отметил, что, получив запрос от потребителей, Kaspersky для своей SIEM-системы безопасности уже внедрил ИИ-консультанта.

ИМПОРТОЗАМЕЩЕНИЕ: ЭТО РЕАЛЬНО?

Цифровой суверенитет Беларуси в области кибербезопасности тоже обсудили. «Создать конкурентоспособный продукт с нуля – это минимум 5-10 лет работы», – отметил один из спикеров. И пока, по мнению участвовавших в дискуссии, разработка собственных средств защиты информации в нашей стране находится на этапе становления. Руководители центров кибербезопасности основными препятствиями для развития разработки называют нехватку экспертизы в области кибербезопасности и высокую конкуренцию с международными вендорами.

КОГО ЗАЩИЩАТЬ?

От технологий, на которых выстраивается инфраструктура защиты от киберугроз, к вопросу формирования абонентской базы.

«Мы призываем компании и особенно те, которым необходимо обеспечить защиту в рамках определенных законодательством сроков, не откладывать с обращением в центры кибербезопасности. Важно понимать, что на подключение объекта необходимо в среднем 4 месяца», – подчеркнул начальник ЦКБ РУП «Национальный центр обмена трафиком» Дмитрий Яворский.

К слову, для небольших компаний и госучреждений тоже уже формируются решения для обеспечения защиты от киберугроз. Центры кибербезопасности предлагают услуги под ключ, включающие аудит, настройку защиты и даже администрирование инфраструктуры. «У малого бизнеса зачастую нет даже сисадмина, не говоря уже о специалисте в области информационной безопасности. Поэтому мы берем на себя все задачи – от прокладки кабелей до мониторинга угроз», – поделился начальник ЦКБ СООО «Мобильные ТелеСистемы» Кирилл Субоч.

«Важно понимать, что мы находимся только в начале пути формирования национальной системы кибербезопасности, – резюмировал представитель ОАЦ Александр Соколов.– Появление почти двух десятков аттестованных центров – фундамент, на котором предстоит выстроить многоуровневую систему защиты. И мы уже видим качественные изменения: растет экспертное сообщество, появляются собственные наработки, формируется культура кибербезопасности на всех уровнях. У нас появилась уверенность, что мы способны противостоять современным киберугрозам». ВС

Анастасия МАНУИЛОВА