Белый дом анонсирует реформу кибербезопасности.

Белый дом разрабатывает новую политику в области киберстрахования, направленную на защиту от катастрофических киберинцидентов. Новая политика должна быть представлена до конца года. Об этом на конференции Black Hat (или хакер в черной шляпе) — хакер, нарушающий компьютерную безопасность ради личной выгоды или из злого умысла.

 Помимо определения злонамеренных хакеров, Black Hat — это также ежегодное мероприятие, проходящее в Лас-Вегасе, штат Невада, и ориентированное на кибербезопасность. Оно объединяет в себе профессионалов и исследователей, чтобы обсудить последние тенденции, уязвимости и методы защиты в цифровом мире.

 Black Hat ориентирована на академические и технические доклады, практические демонстрации уязвимостей и презентации инструментов и технологий для атаки и защиты. Это делает мероприятие очень интересным для специалистов по кибербезопасности и хакеров, которые желают узнать о последних угрозах и новейших методах борьбы.

 В отличии от похожей ежегодной конференции под названием Def Con, также проходящей в Лас-Вегасе, Black Hat считается более официальной конференцией, в то время как Def Con носит скорее неформальный характер и поддерживает более свободную и креативную атмосферу." data-html="true" data-original-title="Black Hat" >Black Hat 2024 заявил Национальный директор по кибербезопасности Гарри Кокер.

Цель новой политики — управлять рисками, а не избегать их. Это необходимо для стабилизации страховых рынков и повышения уровня кибербезопасности в стране. Правительство США хочет подготовиться к возможным киберинцидентам заранее, чтобы не разрабатывать экстренные меры в спешке, когда уже произойдет катастрофа. Такая подготовка должна повысить устойчивость экономики и уверенность на рынке.

Одним из главных вызовов остается недостаток данных для оценки рисков, с чем сталкиваются актуарии — специалисты, оценивающие уровень защиты компаний для страховых полисов. Кокер отметил, что сейчас работа сосредоточена на этом вопросе.

Хотя подробности новой политики пока не раскрываются, представители ONCD подтвердили, что нынешний страховой рынок недостаточно готов к катастрофическим киберинцидентам. Агентства рассматривают различные меры, которые могли бы улучшить национальную кибербезопасность и обеспечить стабильность на рынке.

Рынок киберстрахования уже давно вызывает споры. Эксперты считают, что страховые выплаты могут способствовать росту числа вымогательских атак. Некоторые хакеры даже устанавливают размер выкупа на основе страховых полисов жертв. Кроме того,

продолжаются юридические споры о роли киберстрахования в случае атак, организованных государствами.