ИЗРАИЛЬ СМЯГЧАЕТ ПРАВИЛА ЭКСПОРТА КИБЕРОРУЖИЯ

Дата: 22.08.2019 Автор: Редакция GEOFOR

Рубрика: Ближний Восток

Израиль смягчает правила экспорта наступательного кибероружия, несмотря на обвинения правозащитных и частных организаций в том, что данные технологии используются некоторыми правительствами для шпионажа за политическими противниками и подавления инакомыслия.

Изменение правил Минобороны означает, что компании теперь могут получить льготы по маркетинговой лицензии на продажу некоторых продуктов в конкретные страны.

Израиль, как и другие крупные оборонные экспортеры, внимательно оберегает от посторонних глаз детали своих продаж оружия, а экспортные правила не широко известны, но военные подтвердили, что изменение вступило в силу около года назад.

Специалисты отрасли говорят, что это изменение позволяет ускорить процесс утверждения для продажи кибероружия или шпионских программ, которые используются для взлома электронных устройств и мониторинга онлайн-коммуникаций.

Министерство обороны Израиля заявило, что изменение правил “было сделано для содействия эффективному обслуживанию израильской промышленности при сохранении и защите международных стандартов экспортного контроля и надзора”.

Освобождение от маркетинговой лицензии предоставляется только при “определенных условиях, связанных с разрешением на безопасность продукта и оценкой страны, в которую продукт будет продаваться”, и что компании по-прежнему обязаны иметь экспортную лицензию. Израильское правительство и компании отказались комментировать, какие соседние государства входят в число заказчиков шпионских программ.

В знак того, что власти могут внести больше изменений, министерство экономики, которое отвечает за содействие экономическому росту и экспорту, создает подразделение для обработки экспорта кибертехнологий,

которые имеют наступательные и оборонительные возможности.

“Это часть реформы, которая, по сути, выделяет больше ресурсов министерству экономики на этот важный вопрос”, - сказала пресс-секретарь Министерства.

Передовое кибероружие до недавнего времени применялось только самыми технически совершенными правительственными шпионскими агентствами, такими как США, Израиль, Китай и Россия.

Но теперь появился надежный коммерческий рынок для мощных хакерских инструментов и услуг, а бывшие правительственные киберэксперты из США, Израиля и других стран играют большую роль в торговле.

Это привело к новому подходу в анализе того, как покупается, продается и развертывается кибероружие, а также оценке действий правительств по регулированию торговли. Израильские компании, в том числе NSO Group и Verint, а также оборонный подрядчик Elbit Systems, входят в число мировых лидеров на растущем мировом рынке кибероружия. Программные средства используют уязвимости в мобильных телефонах и других технических продуктах для получения доступа и скрытого мониторинга пользователей.

Некоторые группы по защите частной жизни и правам человека говорят, что контроль Израиля над продажей кибероружия недостаточен. Ранее в этом году Amnesty заявила, что правительство должно принять более жесткую линию против экспортных лицензий, которые “привели к нарушениям прав человека”.

Израильское правительство отказалось комментировать обвинения в нарушении прав человека.

Правозащитные группы говорят, что соседние государства, включая Саудовскую Аравию и Объединенные Арабские Эмираты, являются одними из клиентов шпионских программ израильских фирм.

Дипломатические соображения могут вступить в игру и помочь ускорить продажи. Профессор Тель-Авивского университета Исаак Бен Исраэль, отец киберсектора Израиля и председатель его космического агентства, заявил, что нет ничего плохого в использовании технологий для формирования связей с соседями, которые избегают официальных связей.

”Это законный инструмент дипломатии", - сказал он.

Израильские компании заявляют, что они соблюдают государственные экспортные правила и проверяют клиентов, чтобы обеспечить использование технологии в законных целях иностранными правительствами.

Отметим, что процесс одобрения Израилем экспорта кибероружия является более строгим, чем в некоторых других странах, таких как США и Великобритания.

Рон Дейберт, директор Citizen Lab в Университете Торонто, который фокусируется на цифровом шпионаже и раскрыл предполагаемые шпионские злоупотребления в странах, включая Объединенные Арабские Эмираты и Мексику, сказал, что “жаль”, что Израиль ослабляет свои правила.

"Наше исследование показывает, что существует кризис в гражданском обществе из-за злоупотребления коммерческими шпионскими программами”, - сказал Дейберт Reuters в электронном письме.

В июньском докладе Организации Объединенных Наций содержался призыв к введению глобального моратория на продажу кибероружия до тех пор, пока в Израиле и других странах не будут приняты соответствующие правам человека гарантии.

Во всем мире 42-национальное соглашение об экспорте оружия, известное как Вассенаарские договоренности, охватывает “программное обеспечение для вторжения” и системы интернет-наблюдения. Израиль не является стороной соглашения.

Специальный докладчик Организации Объединенных Наций Дэвид Кей подверг критике контроль Израиля как “окутанный тайной” и призвал к тому, чтобы все продажи кибероружия были обусловлены соблюдением прав человека. Citizen Lab связала программное обеспечение для взлома мобильных телефонов NSO, известное как Pegasus, со шпионскими скандалами в Мексике, Объединенных Арабских Эмиратах и Саудовской Аравии. При этом NSO говорит, что все его продажи одобрены правительством Израиля. Рейснер, который является членом комитета по этике в НСО, сообщил, что компания добровольно отказалась от бизнеса на сумму 200 миллионов долларов между 2016 и 2018 годами.