КИБЕРВОЙНА МЕЖДУ ИЗРАИЛЕМ И ИРАНОМ: РИСКИ И ПЕРСПЕКТИВЫ

Дата: 20.12.2021 Автор: Иван Андрианов

Рубрика: Ближний Восток

В одном из своих недавних материалов эксперты британского аналитического центра The Economist Intelligence Unit (EIU) констатируют, что, по всей видимости, теневая война, которую Израиль и Иран ведут с разной степенью интенсивности на протяжении многих лет, выходит на новый уровень, и обе страны все чаще проводят кибератаки на гражданские объекты друг друга. Тут же правда отмечается, что на сегодняшний день подобные действия лишь несколько раз приводили к неприятным последствиям.

Тем не менее, это может свидетельствовать о растущей способности и готовности обеих стран, и в первую очередь, как подчеркивают британцы, Израиля, наносить не демонстративный, а реальный экономический, инфраструктурный ущерб друг другу.

Как отмечают в EIU, считается, что Израиль и Иран нацелены друг на друга по целому ряду направлений, включая израильские атаки на иранских представителей в Сирии и помехи для судоходства, которые создает Тегеран,в Персидском заливе, наряду с использованием методов кибервойны. Проблема заключается в том, что из-за скрытого характера подобного противостояния, практически невозможно определить, кто же несет ответственность за конкретные кибератаки. Ни одно из правительств в мире публично не признает свою роль в подобных акциях, взломы сетей и серверов часто организуются прокси-группами, которые могут быть и не связаны с правительствами напрямую. Таким образом, нередко получается так, что вина возлагается на третьи стороны. Тем не менее, в последние месяцы наблюдается заметный рост числа кибератак, направленных против гражданских лиц.

Британские эксперты считают, что атаки на израильские объекты, которые были приписаны Ирану или группам, лояльно настроенным по отношению к Тегерану, включали взломы баз данных страховой компании, медицинского учреждения и сайта знакомств ЛГБТК, что привело к публикации личной информации пользователей в Интернете, а также к атаке вымогателей на больницу.

Предполагаемые израильские нападения на иранские объекты были более серьезными и нарушили работу крупного порта и национальной железной дороги. Самый серьезный недавний инцидент, связанный с гражданским объектом, произошел в октябре 2021 года, когда 4300 автозаправочных станций Ирана были заблокированы от приема смарт-карт, субсидируемых государством. Властям потребовалось 12 дней, чтобы восстановить их работу. Подробнее о данном инциденте мы уже писали в одном из наших материалов.

Точкой отсчета начала кибервойны между двумя странами принято считать 2010 год, когда Израилю и США удалось внедрить вирус Stuxnet на компьютеры, задействованные в разработке иранской ядерной программы. Несмотря на отсутствие подробностей, многие эксперты добавляют, что та кибератака, возможно, стала причиной взрыва на иранском объекте в Натанзе в апреле 2021 года.

Согласно оценке EIU, Израиль начал развивать свои возможности в области кибервойны в начале 2000-х годов, и сегодня Институт мира США (USIP,

федеральное агентство США) оценивает его как кибердержаву 2-го уровня вместе с шестью другими странами по всему миру. Тут, правда, стоит заметить, что по «доброй» американской традиции, только США считаются 1-м уровнем. Иран в свою очередь также имеет значительные успехи в данной сфере и уже обладает своими ноу-хау, даже несмотря на то, что начал активную работу по данному направлению лишь после упомянутой атаки 2010 года. USIP оценивает Иран как державу 3-го уровня, которая использует менее сложные инструменты.

На сегодняшний день неясно, что побудило две страны сосредоточить свои усилия именно на гражданских лицах и объектах, но для обеих сторон дополнительная паника, которая может возникнуть в результате поражения гражданских целей, усиливает давление на соответствующие власти, которые теряют поддержку своих избирателей из-за невозможности обеспечить их защиту.

Возможно, зародил эту тенденцию как раз Тегеран после того, как, согласно ряду сообщений, организовал нападение на израильский объект водоснабжения в апреле 2020 года. Атака провалилась, но местные СМИ, в конце концов, обнаружили эту попытку и сообщили о ней. После этого израильское правительство почувствовало себя вынужденным ответить нападением на иранский порт Шахид Раджаи.

Ряд экспертов также полагают, что израильские официальные лица считают, что громкие атаки на Иран, такие как нападения на железные дороги и автозаправочные станции, помогут подорвать поддержку режима Исламской Республики со стороны среднего класса. Израиль, возможно, активизировал свои усилия в свете избрания Эбрахима Раиси, о котором мы уже писали ранее, на пост президента Ирана в середине 2021 года, и попыток США – пока безуспешных – возобновить взаимодействие с Ираном по поводу возрождения «ядерной сделки», которую в одностороннем порядке разорвал Дональд Трамп.

В любом случае, сегодня можно точно констатировать, что и Израиль, и Иран пользуются тем, что гражданские объекты более уязвимы, чем военные и правительственные.

При этом хоть Израиль и является родиной одних из лучших в мире продуктов в сфере кибербезопасности, многие гражданские организации по-прежнему недостаточно защищены несмотря на то, что в их базах данных содержатся конфиденциальные данные, такие как, к примеру, медицинские карты больных. В 2018 году в стране был создан Национальный кибернетический директорат (Israel National Cyber Directorate), чтобы помочь фирмам улучшить свои системы

кибербезопасности, но он не может заставить субъектов частного сектора принимать необходимые защитные меры. Многие просто скрывают нападения, чтобы избежать неловкости и сократить свои расходы на защиту от взломов.

При этом, несомненно, противостояние Ирана и Израиля проходит не только в киберпространстве. Так относительно недавно в Исламской Республике прошли острые дебаты между Корпусом стражей исламской революции (КСИР) и Высшим советом национальной безопасности (ВСНБ) о том, в каком положении находятся иранские военные и представители шиитских милицейских формирований в Сирии на фоне постоянных авиаударов израильской авиации. ВСНБ, основываясь на данных российских военных о том, что число атак израильтян будет только нарастать, предложил сократить численность подразделений КСИР и передислоцировать их.

Также в Тегеране озабочены работой по заключению новой «ядерной сделки» с США и, как отмечают ряд иранских аналитиков, именно после начала переговорного процесса в Вене, случаи авиаударов израильской авиации в Сирии участились.

В данном контексте аналитики Института Ближнего Востока (ИБВ) отмечают, что в Израиле, по всей видимости, крайне скептически относятся к возможностям администрации Байдена по сдерживанию Ирана и намерены действовать самостоятельно, не полагаясь на Вашингтон.

В целом подобный сценарий подтверждает наши прогнозы о том, что Соединенные Штаты будут и далее терять свои позиции среди ключевых союзников на Ближнем Востоке, да и в регионе в целом. И вывод войск, а точнее бегство американцев из Афганистана стало лишь дополнительным триггером для ускорения подобных негативных тенденций для Вашингтона.

Не стоит забывать и противостояние разведывательных ведомств двух стран. Так, в «Моссаде» никогда особо и не скрывали, что на протяжении десятилетий проводят работу на территории третьих стран, в том числе и для того, чтобы сорвать иранскую «ядерную программу».

К примеру, как отмечают в ИБВ, «Моссаду» приписывают убийства иранских ученых-ядерщиков и генералов, нанесение ущерба ядерным объектам и ракетным полигонам. Согласно сообщениям СМИ, с 2007 по 2012 года в Иране были ликвидированы пять ученых, а еще один физик-ядерщик Ферейдуна Аббаси в ходе покушения получил ранения, но выжил, а позднее был назначен главой Организации по атомной энергии Ирана.

12 ноября 2011 года в результате двух взрывов, произошедших на складе боеприпасов в Бигданехе, погибли 27 человек, среди которых был генерал Корпуса стражей исламской революции Хасан Могаддам, считавшийся одной из ключевых фигур в военной сфере страны, а сама база была практически разрушена. 28 ноября 2011 года очередной взрыв произошел на территории ядерного центра в Исфахане, где находились центрифуги для обогащения урана. 12 декабря того же года произошел взрыв на заводе в провинции Йезд. Несмотря на то, что предприятие позиционировалось как металлургическое, израильские СМИ связывают его деятельность с переработкой урана.

27 ноября 2020 года британская газета Jewish Chronicle сообщила, что известный как «отец бомбы» 59-летний Мохсен Фахризаде погиб в результате покушения. Интересно, что при этом ни его охранники, ни члены семьи не пострадали даже, несмотря на то, что атакующие использовали сверхточное автоматическое оружие, управляемое дистанционно, что говорит об их исключительно высоком профессионализме и грамотном планировании операции, а также предшествующей нападению разведывательной работе.

И это лишь небольшой список.

При этом в самом Израиле понимают, что военный метод по уничтожению иранской ядерной программы невозможен. Для этого потребуется прямое участие в конфликте США, что сегодня точно не произойдет.

В данном контексте ряд экспетов из Ирана считают, что наиболее вероятным сценарием будет наращивание диверсионно-разведывательных операций израильских спецслужб как против ядерных объектов, так и ученых. Думается, что в данный список стоит добавить высокопоставленных военных и чиновников, а также объекты гражданской инфраструктуры. Особенно те, что косвенно связаны с разработкой ядерной бомбы. Это могут быть те же заправки, объекты, связанные с электроэнергетикой, транспортом и т.д.

Тем не менее, в Израиле, судя по всему, все же предпринимают попытки заручиться хотя бы косвенной поддержкой американцев, о чем свидетельствует недавний визит главы израильской разведки «Моссад» Давида Барнеа в США. По информации ИБВ, в ходе визита он передал своим американских коллегам досье, в котором содержалась информация о развитии ядерной программы Ирана и объектах, где ведется обогащение урана сверх разрешенной нормы в 20%. По некоторым данным, один из этих объектов расположен на севере Ирана в 50 км от границы с Азербайджаном, а второй объект находится на юге Ирана в провинции

Ахваз на побережье Персидского залива

Однако стоит отметить, даже если учитывать, что Израиль сегодня обладает превосходящими возможностями в вопросах кибербезопасности, уязвимость его гражданского сектора вынуждает власти страны действовать более осмотрительно. Подобный факт несколько развязывает руки иранцам, хотя противостояние все равно на сегодняшний день, хоть и обостряется, но остается взвешенным и контролируемым. По крайней мере, пока остается.

В EIU считают, что в 2022 году существует вероятность того, что Израиль усилит свое давление и количество нападений, особенно учитывая продолжающуюся работу иранцев по развитию своей ядерной программы.

Подобное обострение, вероятнее всего, вынудит Тегеран активнее проводить ответные атаки на гражданские объекты Израиля. Тем более что это, пожалуй, одна из немногих областей, где он может добиться реальных успехов, не прибегая к началу полномасштабных боевых действий.

Если это так, Израиль, несомненно, будет вынужден ответить тем же, что приведет к дальнейшей эскалации нынешнего цикла нападений. Неспособность США возобновить ядерные переговоры с Ираном, вероятно, даст Израилю больше свободы действий на всех фронтах теневой войны, включая кибервойну.

Тем не менее, полноценных военных действий, даже, несмотря на вероятность эскалации конфликта, сегодня ожидать не приходится, хотя риски и возрастут. Это связано, в том числе, с процессом формирования новой системы региональной безопасности на Ближнем Востоке, в которую вовлечены помимо Израиля и Ирана, Турция, Объединенные Арабские Эмираты, Саудовская Аравия, Сирия и даже Ирак, который хоть и находится в полуразрушенном состоянии, но в будущем может стать ключевой страной в новой конфигурации региона, о чем подробнее можно прочитать в нашем материале.