NSO Group Technologies Ltd.

Выпускная квалификационная работа

АВТОРЫ:
Попов В.В., Стойчевич С. и другие ученики курса
«Разведывательный анализ информации»

РУКОВОДИТЕЛЬ ПРОЕКТА:
Ромачев Роман Владимирович

ver. 1.00
20.05.2024

РТЕХНО

*Этот материал подготовлен выпускниками курса «**Разведывательный анализ информации**».*

Автор программы: генеральный директор «Р-Техно» - Ромачев Р.В.

Содержание отчета

Выводы

«NSO Group Technologies Ltd.» – частная израильская компания кибер-разведки, основанная в 2010 году в Израиле Хулио Шалевом (Shalev Hulio), Омри Лави (Omri Lavie) и Нивом Кармы (Niv Carmi), бывшими сотрудниками подразделений израильских вооруженных сил.

«NSO Group» разрабатывает и инструменты кибер-разведки, и другие технологические решения для правоохранительных органов и спецслужб в целях предотвращения угроз общественной безопасности.

Компания создала программные обеспечения **«Eclipse»**, **«Fleming», Landmark»**, самый известный сервис-продукт **«Pegasus»** - систему скрытого наблюдения, служащую интересам Израиля, получившую мировое признание с момента появления на рынке в 2011 году.

«Pegasus» доставляется на телефон бесконтактным путем, обеспечивает удаленный и скрытый мониторинг и полное извлечение данных с устройств с помощью не отслеживаемых команд. Система **«Pegasus»** внесена государством Израиль в категорию «оружие», лицензия на экспорт выдается израильским правительством. «NSO Group» постоянно пиарят свое ПО, представляя эту программу как кибер-разведку для глобальной безопасности и стабильности, в т.ч. для борьбы с криминалом и терроризмом.

Состоящая из множества компаний корпоративная структура **«NSO Group»**, подкрепленная глобальными инвестициями и формируемая стратегическими приоритетами частных инвестиционных фондов и правительств, осуществляет деятельность юрисдикций по всему миру, включая Британские Виргинские острова, Болгарию, Каймановы острова, Кипр, Израиль, Люксембург, Великобританию и США.

Компании в Болгарии и на Кипре проявились как экспортные хабы. Базирующаяся в Люксембурге «Q Cyber Technologies», выступала в качестве коммерческого дистрибьютора, выполняя такие задачи, как маркетинг, подписание контрактов, выставление счетов, и прием платежей от клиентов. Кроме того, «Westbridge Technologies», зарегистрированная в США, потенциально облегчала продажи компании в Соединенных Штатах (на сегодняшний день ликвидирована).

Программное обеспечение «NSO Group» используется многими правительственными структурами по всему миру, включая бывшие страны СССР, а именно Казахстан, Узбекистан, Киргизию, Таджикистан, Азербайджан, Прибалтику.

У компании возникли серьезные репутационные и финансовые проблемы в связи с использованием разведывательного ПО «Pegasus» против гражданских целей силовыми структурами государственных клиентов. В ноябре 2021 года «NSO Group» была внесена в черный список «Департаментом торговли США» и потеряла доступ к американскому рынку.

В начале 2024 года, после судебных исков, «NorthPole», основная компания, владеющая «NSO Group Technologies Ltd», снова оказалась в руках учредителя Омри Лави посредством его люксембургской компании «Dufresne Holdings». Следует отметить, что одним из ключевых исполнительных директоров «NSO Group» на сегодняшний день является англичанка украинского происхождения Тамара Макаренко.

Отсутствие прозрачности в корпоративной структуре «NSO Group» и юрисдикциях, в которых она осуществляет свою деятельность, является существенным препятствием для привлечения к ответственности за предполагаемые нарушения прав человека, связанные с ее продуктами и услугами. Вероятнее всего, это сделано для конспирации разведывательной деятельности.

В настоящий момент «NSO Group» реструктурируется, расширяется, активно лоббирует свое исключение из черного списка «Департамента торговли США» и вкладывает средства в имиджевую реставрацию.

Анализ коммерческой стратегии «NSO Group» показывает, что компания определенно позиционирует себя как неотъемлемый технологический партнер для правительственных органов безопасности, разведки и обороны. Государственным структурам не хватает технологических ресурсов, чтобы справиться с быстрым развитием технологий конечного шифрования, которые предлагают крупные коммерческие компании на рынке и которые активно используются криминальным миром.

Принимая во внимание специфичность продукции, есть все основания полагать, что «NSO Group» и дальше будет вести свою деятельность через сетевых посредников в интересах правительства Израиля, согласие которого необходимо для лицензированного экспорта. Но на этот раз тщательно скрывая имена своих инвесторов и акционеров, которые на данный момент не разглашаются.

В начале 2024 года «NSO Group» официально насчитывала 56 клиентов, в 31 стране, и высказывала намерение расширять свою деятельность в рамках стратегических партнерств с выбранными странами.

Идентификационные данные

Полное наименование компании: NSO Group Technologies Limited
Сокращенное наименование компании: NSO Group

Страна: Израиль
Основание: 12.2009г.
Дата регистрации: 25.01.2010г.
Идентификационный номер: 514395409

Тип организации: Израильская частная компания (Israeli private company)
Форма организации: Частная компания с ограниченной ответственностью

Почтовый адрес: 22 Галгалей Хаплада, Герцлия, Тель-Авив-Яффо, Израиль 4672222 (22 Galgalei Haplada, Herzliya, Tel Aviv-Yafo, Israel 4672222)
Расположение организации: ул. Галгалей ХаПлада, 16, Герцлия, 4672216, Израиль (16 Galgaley HaPlada St. 4672216 Herzelia, Israel)

Официальный сайт: https://www.nsogroup.com (сайт прекратил работу)

Телефон: +972.77.4341292
Факс: +972.77.4253513

Почта: office@nsogroup.com

Социальные сети: https://linkedin.com/company/nso-group

Материнская компания (на 2023 г.): Q Cyber Technologies Ltd (514971522)
Директор: Kew Cyber Technologies Ltd.
Держатель опциона: Ann Group. ace. or. Technologies Ltd. Ann Group. ace. or. Technologies Ltd.
Оборот: 420 миллионов долларов (2020 год)
Число сотрудников на 2023 г.: 600 чел.

«NSO Group» является обобщающим термином и торговой маркой, принадлежащей NSO Group Technologies Ltd. Термин «NSO Group» используется для обозначения различных операционных, финансовых и холдинговых сущностей, находящихся в разных странах и связанных с основной с NSO Group Technologies Ltd.:

- NSO Group Technologies Ltd.
- Q Cyber Technologies Sarl
- Osy Technologies Sarl
- Triangle Holdings Sa

- Square 2 Sarl
- Northpole Holdco Sarl
- Northpole Bidco Sarl
- Northpole Newco Sarl
- Emerald Lie Sarl
- Diamond Lie Sarl
- Goatilev Ltd.
- Ngtp Ltd.
- S. Sesame Technology Ltd.
- Cs - Circles Solutions Ltd.
- Ms Magnet Solutions Ltd.
- Global Hubcom Ltd.
- Mi Compass Ltd.
- Magnet Bulgaria Eood
- Circles Bulgaria Eood

NSO Group в Израиле

NSO Group Technologies ltd. является частной израильской компанией с ограниченной ответственностью, зарегистрированной в Израиле. Именно с NSO Group Technologies ltd. началась мировая коммерческая экспансия NSO Group.

Идентификационный номер компании в Израиле: 514395409.
Сайт компании: https://www.nsogroup.com

Адрес на 22/04/2024: 122 Golgalei Hoplado St. P.D.B 4166, Hertsliya, 4672222, Israel. Но группа NSO заключила договор, сроком на 10 лет (со второй половины 2025 года) на аренду 4-х этажей в новом строящемся здании в Глилот, недалеко от Тель-Авива.
Телефон: +972.77.4341292 | Факс: +972.77.4253513.

NSO Group Technologies Ltd. является дочерней компанией **Q Cyber Technologies Ltd.**

Q Cyber Technologies Ltd. зарегистрирована 02 декабря 2013 в Израиле (идентификационный номер компании в Израиле: 514971522).

Goatilev Ltd. входящая в группу NSO, зарегистрирована в Израиле под номером 516105657. В настоящий момент испытывает трудности, на официальном сайте документы просрочены, компания в процессе реструктуризации или банкротства.

NGTP Ltd. Зарегистрирована в Израиле 20/06/2019 (идентификационный номер компании в Израиле: 516043551), активна.

S. Sesame Technology Ltd. зарегистрирована в Израиле 05/09/2019 (идентификационный номер компании в Израиле: 516080850), активна.

NSO Group в Люксембурге

Торговая марка «Q Cyber Technologies» принадлежит OSY Technologies SARL. OSY Technologies SARL является владельцем интеллектуальной собственности NSO Group Technologies Ltd.

Q Cyber Technologies Ltd., OSY Technologies SARL, Triangle Holdings SA, Square 2 SARL, NorthPole Holdco SARL, NorthPole Bidco SARL, NorthPole Newco SARL зарегистрированы в Люксембурге.
Единый юридический адрес в Люксембурге для Q Cyber Technologies Ltd., OSY Technologies SARL, Triangle Holdings SA, Square 2 SARL: 2, rue Edward Steichen, L-2540 Luxembourg.

Единый юридический адрес в Люксембурге для NorthPole Holdco SARL, NorthPole Bidco SARL, NorthPole Newco SARL: 15, Boulevard F.W. Raiffeisen, 2411 Luxembourg, Luxembourg.

Регистрационный номер в Реестре коммерческих организаций (Luxembourg Business Registers):

- Osy Technologies Sarl - RCS B184226.
- Q Cyber Technologies - RCS B203124.
- Triangle Holdings Sa - RCS B192115.
- Square 2 Sarl Rcs - B192125.
- Northpole Holdco Sarl - RCS B226434.
- Northpole Bidco Sarl - RCS B228505.
- Northpole Newco Sarl - RCS B230411.
- Emerald Lie Sarl - RCS B242289.
- Diamond Lie Sarl - RCS B242326.

Юридический регистрационный номер для купли продажи ценных бумаг (LEI):

- Osy Technologies Sarl 222100KKW3GGPGATJ296 (на 23/04/2024 просрочен).
- Q Cyber Technologies 549300EJG87UMXVFFS58 (на 23/04/2024 просрочен).
- Triangle Holdings Sa 54930042RZ0X284GK323 (на 23/04/2024 просрочен).
- Square 2 Sarl 549300C1372RTHNRIT28 (на 23/04/2024 просрочен).
- Northpole Holdco Sarl 213800RPYA89N1QKSZ13 (на 23/04/2024 просрочен).
- Northpole Bidco Sarl 213800RPYA89N1QKSZ13 (на 23/04/2024 просрочен).
- Northpole Newco Sarl 213800OGDGIJPTK23H63 (на 23/04/2024 просрочен).

- Diamond Lie Sarl RCS 984500FC3A78442CC774 (на 23/04/2024 просрочен).

NSO Group в Англии

С 2023 управляющие компании, связанные с Group NSO, а именно Northpole Holdco SARL, Triangle Holdings SA, Square 2 SARL, Northpole Bidco SARL, Emerald lie SARL перебазировались из Люксембурга в Лондон.

Регистрационный номер в Реестре коммерческих организаций в Англии (company registration number (CRN) в категории холдинговых компаний:

- Triangle Holdings SA FC040779 (документ BR025894 -12/06/ 2023).
- Square 2 Sarl FC040193 (документ BR025303 – 18/11/ 2022).
- Northpole Holdco SARL FC039236 (документ BR024337 – 26/01/ 2022).
- Northpole Bidco SARL FC040113 (документ BR025223 - 18 /11/2022).
- Emerald Lie SARL FC040101 (документ BR025211 - 18 /11/2022).

Единый юридический адрес в Лондоне: 60 Cannon Street, London, EC4N 6NP.

NSO Group на Кипре

CS - Circles Solutions Ltd. зарегистрирована на Кипре 15/10/2014 (идентификационный номер компании на Кипре: HE 336847), активна.

MS Magnet Solutions Ltd. зарегистрирована на Кипре 10/07/2012 (идентификационный номер компании на Кипре: HE 309073), активна.

Global Hubcom Ltd. зарегистрирована на Кипре 18/07/2013 (идентификационный номер компании на Кипре: HE 323665), активна.

MI Compass Ltd. зарегистрирована на Кипре 24/09/2015 (идентификационный номер компании на Кипре: HE 347278), активна.

NSO Group в Болгарии

Magnet Bulgaria EOOD зарегистрирована в Болгарии в апреле 2014 (идентификационный номер компании в Болгарии: 203012611), активна.

Circles Bulgaria EOOD зарегистрирована в Болгарии в июле 2017, активна.

Дополнительно

Circles Bulgaria была учреждена в 2010 году Надеждой Эди-Петровой Роплевой (Nadezhda Edie-Petrova Ropleva, также Nadezhda-Edi Ropleva, также Nadia Ropleva), болгарского происхождения проживающей в Израиле. Бывшее название компании – «Данида». Затем являлась дочерней компанией кипрской оффшорной компании «CS - Circles Solutions Ltd.» принадлежащей NSO Group.

Действующий Главный директор Circles Bulgaria EOOD по клиентским отношениям Александэр Пенков (Alexander Penkov), не афиширует в своем профессиональном профиле свою причастность к компании. Профайл Нади Роплевой больше не доступен в LinkedIn, но Flo Live регулярно цитирует ее имя.

Надя Роплева является на сегодняшний день Директором Flo Live в Болгарии. Flo Live Ltd. была создана в 2015 году в Англии (09931232), затем была создана дочерняя Flo Live Israel Ltd. в 2016 г. На начало 2023 г. у Flo Live Ltd. имелись дочерние компании в США, Израиле, Кипре, Англии, Болгарии, Сингапуре, Турции, на о. Гернси.

Согласно Forensic News Flo Live и Circles Bulgaria тесно связаны, и компания Flo Live является прикрытием для хакеров и частных разведчиков, стоящих за Circles.
В сентябре 2023 г. Flo Live заявила о новых инвесторах Greenfield Partners (израильская инвестиционная компания) и 83North (английский инвестиционный фонд). Таким образом прослеживается связь между Flo Live и Circles.

Справочно

На сегодняшний 100% акций всех вышеперечисленных компаний, а значит и NSO Group Technologies Ltd. передано кредиторами Dufresne Holding.

Dufresne Holding основана в Люксембурге основателем NSO Group Technologies Ltd. Омри Лави и зарегистрирована в Реестре коммерческих организаций 10 февраля 2023г.

Регистрационный номер в Реестре коммерческих организаций (Luxembourg Business Registers): RCS B275054.

Адрес: 2, rue Edward Steichen, L-2540 Luxembourg.

История становления компании

2009 год

В феврале 2009 года Ронен Сасон (Ronen Sasson), Эран Ларпен (Eran Karpen), а также Шалев Хулио (Shalev Hulio) и Омри Лави (Omri Lavie), знакомые со школьной скамьи, основали компанию CommuniTake Technologies, которая изначально предлагала технологию авторизированного дистанционного доступа к мобильным телефонам для сотрудников технической поддержки производителей. Интерес разведывательных сообществ к дистанционному доступу и перспективы работы с государственными клиентами, мотивировал выход Шалев Хулио и Омри Лави из CommuniTake Technologies с целью создания технологии неавторизированного доступа для государственных заказчиков.

2010 год

25 января 2010 года Нив Карми (Niv Carmi), Шалев Хулио (Shalev Hulio) et и Омри Лави (Omri Lavie) создают компанию NSO Group Technologies Ltd, NSO Group. Инициалы их имен образуют аббревиатуру NSO. Трое основателей и первые стратегические советники NSO Group – ветераны израильской армии. Шалев Хулио служил майором в поисково-спасательном подразделении израильской армии, Омри Лави, в артиллерии. Нив Карми служил как в военной разведке, так и в Моссаде. Старший советник Даниэль Рейснер (Daniel Reisner) ранее занимал должность руководителя Международного правового отдела израильской армии и был ответственным за консультирование израильского руководства по израильско-палестинским отношениям и антитеррористическим операциям. Буки Кармели (Buky Carmeli), еще один старший советник, является бывшим руководителем подразделения кибербезопасности Министерства обороны Израиля (IMOD).

Каждый член компании NSO являлся или является ветераном разведывательных служб, большинство из них служили в AMAN, Дирекции военной разведки Израиля, многие в подразделения Unit 8200, разведке по кибербезопасности. Самые ценные сотрудники компании — выпускники элитных учебных курсов и заведений, включая секретную и престижную программу Unit8200 под названием ARAM, которая принимает несколько самых блестящих студентов и обучает их самым передовым методам программирования кибероружия.

Разработанный ими в 2010 году инструмент, который они назвали Pegasus, предлагал комплексное решение сбора как секретной, так и личной информации для разведывательных служб и полиции, которые не могли позволить себе разрабатывать собственные инструменты. Цель, говорилось в описании, состояла в том, чтобы продать

этот инструмент этим заказчикам, которые бы использовали его для борьбы со всеми видами преступности, от терроризма до отмывания денег и незаконного оборота наркотиков по всему миру.

Стартап методично внедрялся в растущий мир кибер-слежки, за считанные годы превратившись из начинающего претендента в бизнес–гиганта. Мексика стала одним из первых клиентов, готовым потратить невероятные суммы денег на подобные технологии.

2012 год

Компания получила первый крупный контракт на 20 миллионов долларов от правительства Мексики, которое наняло ее службы для борьбы с незаконным оборотом наркотиков.

2013 год

Годовой доход компании составил около 40 миллионов долларов США.

2014 год

NSO Group была приобретена за 130 миллионов долларов американской инвестиционной компанией Francisco Partners, специализирующейся на инвестициях в технологический сектор.

Компания Circles была приобретена за 130 миллионов долларов американской инвестиционной компанией Francisco Partners и объединилась с NSO Group, Появление одноименного ПО Circles, который позволяет установить местоположение смартфона в любой точке мира в течение секунд.

2015 год

Годовой доход составил около 150 миллионов долларов.

Francisco Partners пытался продать компанию на сумму до 1 миллиарда долларов.

Компания продает технологию видеонаблюдения правительству Панамы. Позже контракт стал предметом панамского антикоррупционного расследования после того, как

он был раскрыт в результате утечки конфиденциальной информации из итальянской фирмы Hacking Team.

2016 год

В августе 2016 года NSO (через свою американскую дочернюю компанию Westbridge) представила американскую версию Pegasus Департаменту полиции Сан-Диего (SDPD). В маркетинговом материале Westbridge подчеркнула, что компания базируется в США и контрольный пакет акций принадлежит американской материнской компании.

Примерно в 2016 году NSO, по сообщениям, продало программное обеспечение Pegasus в Гану.

2017 год

В июне 2017 года компания Francisco Partners выставила на продажу NSO Group более чем за 1 миллиард долларов (что примерно в десять раз превышает первоначальную сумму, которую Francisco заплатила за ее приобретение в 2014 году). На момент выставления на продажу в NSO работало почти 500 сотрудников (по сравнению с примерно 50 в 2014 году).

Израильские СМИ сообщили, что Blackstone Group ведет переговоры о покупке части NSO. Однако позже источники сообщили Reuters, что американская частная инвестиционная компания вышла из этих обсуждений месяц спустя.

Компания оказалась в центре внимания на фоне утверждений о том, что правительство Мексики использовало разведывательное ПО Pegasus Mobile компании с целью дискредитации частных лиц.

В июле переговоры с американской компанией-разработчиком программного обеспечения Verint Systems о слиянии ее подразделения безопасности с NSO стоимостью около 1 миллиарда долларов завершились без достижения соглашения.

2018 год

На NSO Group посыпались обвинения в злоупотреблениях. Правозащитная группа Amnesty International обвинила NSO в том, что она помогала Саудовской Аравии скрытно наблюдать за личной жизнью одного из сотрудников организации.

Летом 2018 года несколько мексиканских журналистов, включая Кармен Аристеги, подали судебную жалобу на NSO в Израиле. Компанию обвинили в причастности к убийству саудовского журналиста и диссидента в Турции, но NSO Group отрицала какую-либо причастность.

В июне 2018 года израильский суд предъявил бывшему сотруднику NSO обвинение в краже копии Pegasus и попытке продать ее онлайн за 50 миллионов долларов в криптовалюте.

2019 год

В апреле 2019 года NSO заморозила свои сделки с Саудовской Аравией из-за скандала, связанного с обвинениями NSO в отслеживании убийства журналиста Джамаля Хашогги за несколько месяцев до его смерти.

В мае WhatsApp заявил, что NSO Group разработала вредоносное ПО для установки разведывательного ПО на устройство объекта, нацеленного на его функцию вызова в виде сброса звонка.

В июне NSO приступило к созданию испытательного центра в Нью-Джерси для ФБР, которое заказало услуги NSO. ФБР приступило к тестированию версии Pegasus, разработанной для правительственных учреждений США и предназначенной для использования на американских устройствах. ФБР также приобрело ограниченную лицензию на Pegasus, хотя и заявило, что никогда не использовало Pegasus в своих расследованиях и просто стремилось изучить программное обеспечение для наблюдения.

NSO Group столкнулась с пристальным вниманием со стороны правозащитных организаций и была вовлечена в обмен публичными письмами с Amnesty International. Компанию обвинили в продаже своих инструментов правительствам, которые, как считалось, были ответственны за выбор целей, включая Азербайджан, Бахрейн, Казахстан, Мексику, Марокко, Руанду, Саудовскую Аравию, Венгрию, Индию и Объединенные Арабские Эмираты.

14 февраля Francisco Partners продала контрольный пакет акций (60%) NSO обратно соучредителям Шалеву Хулио и Омри Лави, которые были поддержаны в покупке европейским фондом прямых инвестиций Novalpina Capital, специализирующимся на инвестициях в спорные компании. Хулио и Лави инвестировали 100 миллионов долларов, а Novalpina приобрела оставшуюся часть контрольного пакета акций, таким образом, компания была оценена примерно в 1 миллиард долларов. На следующий день после приобретения Novalpina попыталась решить проблемы, поднятые Citizen Lab о

разведывательном предназначении продуктов NSO, направив письмо, заявляя о своей уверенности в том, что компания действует достаточно добросовестно и осторожно.

2020 год

NSO Group закрыла кипрские офисы Circles, компании, которую она приобрела в 2014 году. В статье, основанной на интервью с двумя бывшими сотрудниками, интеграция между двумя компаниями описывалась как «ужасная» и говорилось, что вместо этого NSO будет полагаться на болгарский офис Circles.

В апреле 2020 года Motherboard сообщила об инциденте, произошедшем за несколько лет до этого, когда сотрудник NSO использовал инструмент Pegasus против клиента для слежки за изменой (личной знакомой женщиной) во время рабочей поездки в ОАЭ. Сотрудник проник в офис клиента в нерабочее время, чтобы воспользоваться инструментом, что вызвало тревогу и расследование со стороны клиента. По словам источников Motherboard, сотрудник был задержан властями и уволен из NSO.

В июле 2020 года в СМИ появилась информация от агентства Motherboard, которое сообщило, что американское отделение NSO в течение 2018 года предлагало Секретной службе США свой бренд Pegasus.

2021 год

В 2021 году NSO Group стала объектом журналистского расследования. Представителей компании обвинили в продаже разведывательного ПО авторитарным правительствам, слежке за журналистами и общественными деятелями. Вследствие этого Администрация президента США Байдена внесла NSO Group в черный список (Entity list) компаний, которым запрещено поставлять (экспортировать) американские технологии. Это был больше имиджевый ход, направленный на создание финансовых проблем у NSO Group с целью ее дальнейшей покупки, писали в СМИ.

В декабре 2021 года 86 правозащитных организаций направили совместное письмо с призывом к ЕС ввести глобальные санкции против NSO Group и добиваться «запрета продажи, передачи, экспорта и импорта технологий наблюдения израильской компании» из-за рисков, которые технологии NSO представляют для прав человека во всем мире.

2022 год

Вскоре после расследования представители одной из основных подрядных организаций Пентагона, компании L3Harris Technologies, сообщили своим коллегам из NSO Group, что они получили поддержку правительства и американской разведки на приобретение компании, если исходный код Pegasus и кэш обнаруженных уязвимостей будут переданы другим спецслужбам англосаксонского разведсообщества Five Eyes.

Формально, внесение компании в Entity list накладывает запрет только на экспортные операции, связанные с поставками технологий. Но не касается импортных операций или поглощений. Именно на это и рассчитывали представители L3Harris.

2023 год

В процесс включились другие игроки. Кредиторы, включая Credit Suisse и Senator Investment Group, в начале 2023 обратили взыскание на материнскую компанию NSO Group. В результате поглощения была произведена смена владельцев NSO, включая фонд прямых инвестиций, основанный Novalpina Capital, который приобрел компанию в ходе сделки, оценив ее примерно в 1 миллиард долларов в 2019 году.

На осень 2023 г компания Dufresne Holdings, контролируемая соучредителем NSO Group Омри Лави, в корпоративных документах указана в качестве единственного акционера материнской компании NSO Group. Представители этой компании принимают активное участие в управлении NSO Group. По их инициативе были уволены некоторые сотрудники. Тем временем кредиторы NSO Group сотрудничают с Лави и договорились не добиваться от NSO дефолта по долгам.

По словам представителя компании, NSO Group управляется непосредственно генеральным директором Яроном Шохатом, а ее кредиторы в настоящее время занимаются реструктуризацией долей акционеров.

Осенью 2023 года шло, по сути, переоформление активов на новое юрлицо и оптимизация компании, что необходимо для привлечения новых инвестиций и получения чистых регистрационных документов без упоминаний про внесение в черный список. Предполагается, что в любом случае NSO Group, даже в новой оболочке, останется под контролем крупных банков.

Собственники и ключевые лица

С начала основания компания не раз переходила из рук в руки, и множество лиц выступили в качестве ключевых или важных, в зависимости от этапа развития и финансирования компании NSO Group Technologies Ltd. В общем их можно отнести к частным акционерам, инвесторам и менеджерам высшего звена. Так, к примеру, уставы компаний различают два класса директоров А и Б с разным уровнем полномочий.

На момент подготовки материала акционерами являются:

- Омри Лави, соучредитель NSO. Group Technologies Ltd. и директор Dufresne Holdings, компании, владеющей 100% пакетом акций NSO Group Technologies Ltd. переданными синдикатом кредиторов.
- Группа неизвестных инвесторов.

Справочно

В 2023 году медиа- источники указывали на тот факт, что Омри Лави завладел 100% акций NSO Group, будучи 100% акционером Dufresne Holdings. Однако этот этап следует рассматривать как промежуточный, в рамках судебных баталий, реорганизации, оптимизации финансирования и новой группой инвесторов.

На начало 2024 года к важным фигурами можно отнести:

- Ярон Шохат (Yaron Shohat), Генеральный директор NSO. Group Technologies Ltd.
- Джеймс Уорд (James Ward) и Тамара Макаренко (Tamara Makarenko), исполняющие директоры компаний NSO Group, зарегистрированных в Англии и Люксембурге.
- Triangle Holdings SA (идентификационный N° FC 040779), Англия.
- Square 2 SARL. (идентификационный N° FC 040193), Англия.
- Northpole Bidco SARL (идентификационный N° FC 040113), Англия.
- Emerald Lie SARL (идентификационный N° FC 040101), Англия.
- Diamond Lie SARL (идентификационный N° FC 040103), Англия.
- Northpole Holdco SARL (идентификационный N° FC 039236), Англия.
- Q Cyber Technologies SÀRL, Luxembourg.
- Шмуэль Санрай (Shmuel Sunray), главный экспертный юрист NSO. Group Technologies Ltd.
- Тимоти Дикинсон (Timothy Dickinson), лоббист партнер юридической фирмы.
- Paul Hastings (контактное звено с секретарем Энтони Блинкеном (Antony Blinken) для удаления из черного списка).
- Антони Леви (Anthony Levi), поверенный в делах адвокат NSO Group, а также исполняющий директор в компаниях NSO Group:
- IOTA Holdings Ltd., Кипр (на сегодня ликвидирована);
- MI Compass Ltd., Кипр;
- CS - Circles Solutions Ltd., Кипр;

- Global hubcom Ltd., Кипр;
- CI - Compass Ltd., Кипр;
- Q Cyber Technologies SÀRL, Luxembourg.

Дополнительно:

- Гамильтон Блакней (Hamilton Blakeney) и Ашер Алэн Борнстейн (Asher Alain Bornstein) исполняющие директора компаний NSO Group зарегистрированных в Люксембурге.
- Q Cyber Eechnologies SÀRL, Luxembourg (данные на конец 2023 г.).
- Эран Горев (Eran Gorev), партнер операционного управления Francisco Partners, исполнительный и генеральный директор компаний, контролирующих NSO Group Technologies, в 2014 имел 0,8% акций Triangle Holdings SA. Подтвердить или опровергнуть их наличие на сегодняшний день не удалось;
- Кевин Вильсон (Kevin Wilson), бывший сотрудник, является текущим акционером в Triangle Holdings (данные на конец 2021 г.);
- Эдди Шалев, первоначальный инвестор NSO Group Technologies Ltd. (владел в 2014 1,8% акций Triangle Holdings SA, контролирующая NSO Group Technologies). Подтвердить или опровергнуть их наличие на сегодняшний день не удалось;
- Алексей Вороновицкий (Alexei Voronovitsky), бывший инженер-программист в Израильских оборонных силах. Имел 0,1% акций в 2014 году. По официальным данным, Алексей Вороновицкий окончательно покинул компанию и больше не является акционером.

Основатели

Нив Кармi (Niv Carmi). Нив Карми, хотя и покинул компанию вскоре после ее основания, привнес в NSO Group значительный технический опыт. Как у бывшего сотрудника разведки Моссад и эксперта по безопасности, знания и навыки Карми в области кибербезопасности и разведки имели решающее значение на ранних этапах развития компании.

Шалев Хулио (Shalev Hulio) - Шалев Хулио, соучредитель и генеральный директор NSO Group, привносит в компанию сочетание технических знаний и деловой хватки. Его навыки ведения переговоров и бизнес-стратегии сыграли решающую роль в заключении контрактов на миллионы долларов для NSO Group. Лидерство и дальновидность Хулио сыграли ключевую роль в позиционировании NSO Group как ведущего игрока на рынке кибер-разведки. Его приверженность миссии компании, несмотря на судебные тяжбы и разногласия, демонстрирует его стойкость и решительность.

Свое отношение к бизнесу NSO Group Хулио четко высказал в интервью MIT Technology Review: «Люди не понимают, как работает разведка, - сказал Хулио. - Это непросто. Это неприятно. Разведка - дерьмовый бизнес, полный этических дилемм».

Омри Лави (Omri Lavie) - предприниматель и инвестор. Один из основателей NSO Group и руководитель развития бизнеса NSO по всему миру, возглавлял представительство NSO Group в США и был ее первым генеральным директором. В настоящее время является генеральным директором Orchestra Group, целостной платформы кибербезопасности для проактивной киберзащиты, а также соучредителем и управляющим партнером Founders Group, частной инвестиционной компании, которая инвестирует в стартапы на ранних стадиях. Он также является активным филантропом, постоянно поддерживая многочисленные некоммерческие организации в области образования, лечения онкологических заболеваний, ухода за пожилыми людьми и детьми.

Шмуэль Санрай (Shmuel Sunray) - главный юрист NSO Group Technologies Ltd.

Был исполнительным вице-президентом, главным юристом в Rafael Advanced Defense Systems, а также в IMI Systems Ltd. Шмуэль Санрай присоединился к компании Francisco Partners в 2019 году.

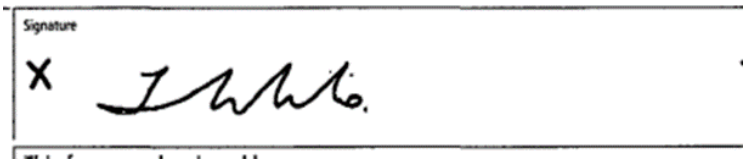
Ярон Шохат (Yaron Shohat) - генеральный директор NSO Group Technologies Ltd.

Получил степень бакалавра по электротехнике в Технионе - Израильском институте технологий в 1992 году, степень магистра делового администрирования в Факультете менеджмента Реканати Университета Тель-Авива в 1998 году. Был Главным операционным директором в компании Nice Actimize, Генеральным директором онлайн-угроз в компании RSA, подразделении по безопасности корпорации EMC. С 2018 году Ярон Шохат работал в инвестиционной компании Francisco Partners.

Тамара Макаренко (Tamara Makarenko), исполнительный директор компаний NSO Group.

Эксперт по разведанализу и политическим рискам. Начальная карьера в государственной сфере. Проведение брифингов для национальных правоохранительных органов, военных, служб безопасности, а также для соответствующих международных организаций, включая Интерпол, Европол, НАТО, ОБСЕ и Совет Безопасности ООН. Опыт в разработке и контроле внутренних расследований, порученных советом директоров и/или акционерами. Степень доктора философии в международной политике от Университета Уэльса (Аберистуит), степень магистра литературы в области международных исследований по безопасности от Университета Сент-Эндрюса и степень бакалавра по политологии от Университета Манитобы. Она говорит на украинском языке и имеет базовые знания французского, немецкого, греческого и русского языков. Является учредителем Faltress Limited в Лондоне.

Подпись на многих финансовых отчетных документов NSO Group в Лондоне.



Микаэль Бетито (Michael Betito), член Совета директоров.
Специалист по инвестициям в iCON Infrastructure с опытом работы в сфере прямых инвестиций и слияний и поглощений.

Специализация: Слияния и поглощения, LBO, Финансирование с привлечением заемных средств, прямые инвестиции, финансовое моделирование, изучение рынка.

Управляющий директор Navalpino Capital, европейского фонда прямых инвестиций среднего бизнеса. Специализируется на здравоохранении (Laboratoire XO), технологиях (NSO) и поставках во Францию. Предыдущий опыт работы в Oaktree Capital (Европейская основная группа) и Goldman Sachs (слияния и поглощения / LevFin).

Образование: Бизнес-школа ESSEC, Высшая школа экономики, Финансы.

Стивен Пил (Stephen Peel), член Совета директоров.
Член попечительского совета Благотворительного фонда больницы Королевского колледжа, Лондон, Великобритания. Председатель попечительского совета Infinity Boat Club, Великобритания. Член Правления Ampowr (Switch the Flick™) - Integrated Battery Energy Storage Systems. Нидерланды. Член организации The Trilateral Commission.

Справочно: Трехсторонняя комиссия (англ. Trilateral Commission) - неправительственная международная организация, состоящая из представителей Северной Америки, Западной Европы и Азии (в лице Японии и Южной Кореи), официальная цель которой — обсуждение и поиск решений мировых проблем. Организация была создана в 1973 году по инициативе ведущей группы Бильдербергского клуба и Совета по международным отношениям, в том числе Дэвида Рокфеллера, Генри Киссинджера и Збигнева Бжезинского.

Образование: Йельский университет (Yale University), степень магистра, Международные отношения. Кембриджский университет (University of Cambridge), степень магистра.

Илана Сарфати (Ilana Sarfati), член Совета директоров.

Директор по исследованиям и разработкам с более чем 20-летним опытом работы, в том числе более 10 лет в управлении сильными, наделенными полномочиями командами разработчиков программного обеспечения. Энергичный и ориентированный на результат лидер, зарекомендовавший себя в предоставлении высококачественных E2E-решений.

В настоящее время руководит 7 командами (более 40 инженеров).

Образование: Технион - Израильский технологический институт, степень бакалавра в области компьютерных наук. Еврейский университет в Иерусалиме, магистр делового администрирования - MBA, Бизнес (MBA).

Ифа Идисис (Yifa Idisis), старший финансовый директор (CFO).

Более чем 20-летний опыт работы в сфере управления финансами по всему миру. В 2015 году присоединилась к NSO, в период, когда она вступила в период стремительного глобального роста.

Навыки:

- глобальное лидерство и командообразование;
- бизнес и коммерческое слияние, и поглощения;
- стратегическое финансовое планирование;
- финансовое прогнозирование и анализ;
- управление эксплуатацией быстрого роста;
- навыки решения проблем и интеграции, сотрудничества заинтересованных сторон;
- отличные коммуникативные навыки, большой опыт создания надежных систем ВИС & акции предложения.

Возглавляла отдел бухгалтерского учета и контроллинга в DHL. Ифа Идисис присоединилась к Francisco Partners в 2013 году.
Образование: получила степень бакалавра в области бухгалтерского учета и экономики в Тель-Авивском университете в 1999 году и степень магистра делового администрирования в области делового администрирования и менеджмента в Тель-Авивском университете в 2004 году.

Орен Меймон (Oren Maymon), главный операционный директор (COO).

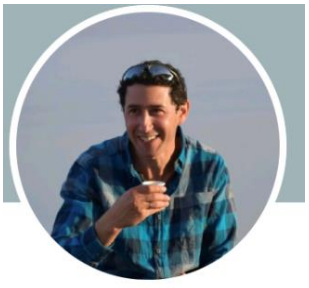
В компании с марта 2020 года. 15-летний опыт работы в качестве исполнительного директора и топ-менеджера высшего звена в публичных компаниях с двусторонней торговлей. Орен был главным операционным директором в Scodix и главным операционным директором в EndyMed Medical Ltd. Орен Меймон присоединился к Francisco Partners в 2020 году.

Навыки:

- 25 лет работы по всему миру, глобальной поддержки клиентов, глобального управления бизнесом и переговоров в качестве главного операционного директора (COO) в ведущих компаниях отрасли;
- огромный опыт управления производственными мощностями по всему миру, как малыми, так и большими объемами, а также очень сложными процессами;
- обширный опыт в управлении глобальными операциями на рабочих местах (управление недвижимостью, контракты, повседневные операции и оборудование);
- близкое знакомство и опыт работы с большинством EMS (Electronic Manufacturing Service) в мире;
- ведение переговоров, заключение и исполнение контрактов на поставку и эксплуатацию;
- постоянное планирование материалов и контроль поставок в очень сжатые сроки, что обеспечивает компании полную гибкость в ведении бизнеса;
- планирование и контроль бюджета компании, включая мониторинг движения денежных средств;
- опыт работы в области корпоративного управления и стратегии;
- определение общих процедур компании, а также соответствие требованиям SOX;
- сильная технологическая подготовка и понимание тенденций рынка;
- отличные навыки общения с людьми.

Образование: Орен Маймон получил степень бакалавра искусств в области бизнеса и менеджмента в Академическом колледже менеджмента в 2010 году и степень магистра делового администрирования в области информационных систем управления в Академическом колледже менеджмента в 2020 году.

Рамон Эшкар (Ramon Eshkar), вице-президент.



В компании с 2015 года.

Руководит значимыми проектами по работе с ключевыми клиентами. Интегрирует корпоративные решения в существующие сети клиентов и помогает в разработке новых

сервисов. Обладает обширным опытом в управлении проектами по работе с различными клиентами по всему миру.

Имеет серьезный опыт работы в передовых международных компаниях в сфере IT. Работал управляющим проектами в Allot Ltd. (NASDAQ: ALLT, TASE: ALLT) - ведущем поставщике инновационных решений в области сетевого анализа и конвергентной безопасности для поставщиков услуг и предприятий по всему миру. Мультисервисные платформы Allot используются более чем 500 поставщиками мобильных, фиксированных и облачных услуг и более чем 1000 предприятиями.

Также имеет опыт работы в качестве управляющего проектами в компаниях Alvarion Technologies - мировой поставщик автономных сетей Wi-Fi и Ribbon Communications (Nasdaq: RBBN) - предоставляет глобальное коммуникационное программное обеспечение и решения для пакетных и оптических сетей поставщикам услуг, предприятиям и секторам критически важной инфраструктуры.

Образование: закончил одно из старейших учебных заведений Израиля - Академический центр Руппина Академический центр, Нетания. Степень E. B.A., бизнес-администрирование.

Кадровая политика компании

В компании существует строгий процесс собеседования, который включает в себя проверку технических знаний и поведенческие вопросы о прошлом опыте. Компания нанимает профессионалов из самых разных областей, включая ученых, инженеров, преподавателей, специалистов в области информационных технологий, специалистов по связям с общественностью, менеджеров, писателей, дизайнеров, бизнес-профессионалов и административный персонал. NSO Group стремится к разнообразию и не допускает дискриминации по признаку расы, пола, цвета кожи, возраста, религии, национального происхождения, сексуальной ориентации, гендерной идентичности или самовыражения, законной политической принадлежности, статуса ветерана, умственных или физических недостатков.

Несмотря на то, что компания столкнулась с несколькими обвинениями и судебными исками, она сохраняет позитивный настрой на развитие бизнеса. Согласно анонимным отзывам сотрудников, 88% сотрудников порекомендовали бы работу в NSO Group своим друзьям, а 86% сотрудников считают, что у NSO Group позитивный настрой на развитие бизнеса. На основе анонимных отзывов компания получила оценку 4,1 из 5 звезд.

Конкретная информация о текучести кадров в NSO Group не является общедоступной. Однако анонимный отзыв на Glassdoor свидетельствует о том, что уровень текучести

кадров в NSO Group высок. В обзоре говорится, что, если сотрудник проработал в компании более года, он считается старшим сотрудником, что означает, что многие сотрудники покидают компанию в течение первого года работы. Это говорит о высокой текучести кадров, хотя точный процент не указан.

За последние годы численность персонала NSO Group увеличилась. В 2014 году в компании работало около 50 сотрудников, но к июню 2017 года это число увеличилось почти до 500. Однако совсем недавно NSO Group была вынуждена уволить 100 из своих 700 сотрудников, что указывает на то, что в настоящее время численность персонала составляет около 600 человек.

NSO Group считает, что счастливые и талантливые сотрудники являются ключом к их успеху, и стремится создать для сотрудников приятный опыт и приятную атмосферу в офисе. Они предлагают длинный список преимуществ, включая медицинское обслуживание для всей семьи, рабочий смартфон, абонементы в тренажерный зал и спортивные мероприятия, транспорт и командные соревнования.

Что касается компенсации, NSO Group предлагает своим сотрудникам опционы на акции, не соответствующие требованиям (NSO). Эти опционы позволяют сотрудникам покупать акции компании по заранее установленной цене, привязывая часть своей компенсации к росту компании. Однако условия опционов могут требовать от сотрудников определенного периода времени, пока они не вступят в силу.

NSO Group также предлагает комплексные и конкурентоспособные льготы и компенсационный пакет, включая полный план медицинского обслуживания и страхования, выход на пенсию, финансовые вознаграждения и льготы,

оздоровительные ресурсы и решения для обеспечения баланса между работой и личной жизнью.

Уровень заработной платы в NSO Group может варьироваться в зависимости от должности, отдела, местоположения, а также уровня образования, сертификатов и других навыков сотрудника. Например, разработчику серверного программного обеспечения в NSO Group платят от 93 754 до 114 454 долларов в год. Предполагаемый диапазон зарплат в сфере розничной и оптовой торговли, где находится NSO Group, составляет от 65 112 до 84 383 долларов, при этом средняя заработная плата составляет около 74 132 долларов. Однако важно отметить, что это приблизительные данные, и фактическая заработная плата может варьироваться.

В Соединенных Штатах общая зарплата сотрудников NSO Group, по оценкам, составляет 137 394 доллара в год при средней заработной плате в 118 052 доллара в год. Эти цифры представляют собой медиану, которая является средней точкой диапазонов, основанных на зарплатах, полученных от пользователей.

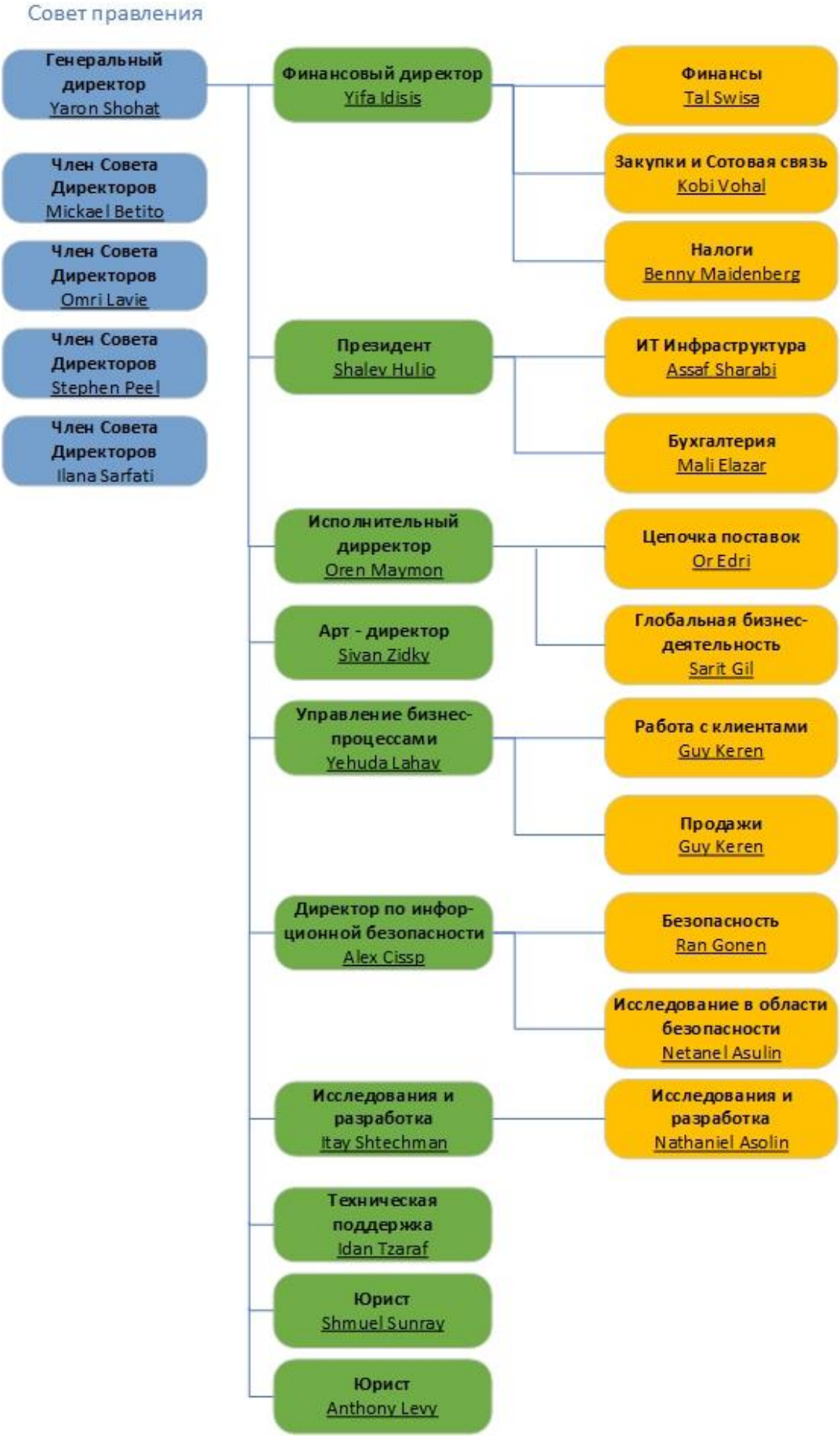
В дополнение к заработной плате сотрудники NSO Group могут также получать другие виды вознаграждения, такие как денежные премии, бонусы за акции, участие в прибылях, комиссионные с продаж и чаевые.

Организационная структура управления компанией

NSO Group - компания, которая разрабатывает инструменты, помогающие правительственным учреждениям выявлять и предотвращать терроризм и преступления, что накладывает на нее определенные обязательства по минимизации информации о структуре компании и ее внутренней иерархии.

NSO Group - компания со сложной корпоративной структурой. Структура управления компанией со временем претерпела изменения, и ключевые руководящие должности стали занимать разные люди. Например, в августе 2022 года тогдашний генеральный директор Шалев Хулио ушел в отставку, а его преемником был назначен главный операционный директор Ярон Шохат. После принудительной реструктуризации, проведенной кредиторами, в мае 2023 года новым владельцем NSO вновь стал соучредитель Омри Лави.

Управленческая структура компании (апрель 2024 года)



Структура компании состоит из различных управлений или департаментов, каждый из которых отвечает за определенную сферу бизнеса.

Конкретная структура компании периодически варьируется и может быть адаптирована в зависимости от потребностей и ее стратегических целей.

Хотя точные подразделения NSO Group не публикуются, есть основания полагать, что они, включают такие отделения, как:

- **Операционный**. Этот отдел может отвечать за повседневное ведение бизнеса.
- **Внешняя разведка.** Этот отдел может сосредоточиться на сборе и анализе информации, относящейся к продуктам и услугам компании.
- **Внешняя безопасность.** Этому отделу может быть поручено обеспечивать сохранность активов компании.
- **Внутренняя безопасность.** Этот отдел может сосредоточиться на защите информационной и технологической инфраструктуры компании.
- **Финансы и администрация.** Этот отдел, скорее всего, будет заниматься финансовыми вопросами компании, включая составление бюджета, финансовую отчетность и расчет заработной платы.
- **Юридические услуги.** Этот отдел будет заниматься юридическими вопросами, заключением контрактов и соблюдением законов и нормативных актов.
- **Исследования и разработки.** Этот отдел или команда будет заниматься разработкой и совершенствованием продуктов компании.

Также стоит отметить, что продукты NSO Group разрабатываются экспертами в области телекоммуникаций и разведки, что позволяет предположить, что в компании, скорее всего, есть отделы или команды, занимающиеся разработкой и тестированием продуктов.

Доходы и источники финансирования NSO GROUP

Финансирование имеет сложную финансово-правовую структуру, в которой сочетаются европейский, американский, израильский и арабский капиталы. В общем основными инвесторами капитала на разных этапах были следующие юридические лица:

- Genesis Partners, инвестиционная венчурная израильская компания.
- Francisco Partners, инвестиционная специализированная американская компания.
- ESOP Management and Trust Services Ltd., инвестиционная израильская копания по Управлению акционерными программами.
- Global Seven Group LP, инвестиционная компания, зарегистрированная на Британских островах.
- Novalpina Capital, холдинговая европейская частная компания.
- CNP Assurances.
- The Centrica Combined Common Investment Fund.
- TREO Asset Management, инвестиционная американская компания.
- Mubadala Capital (Mubadala Investment Company PJSC), холдинговая компания пренадлежащая правительству Абу-Даби.

- The Oregon Public Pension Fund, пенсионный фонд штата Орегон, официально известный как Орегонская система пенсий государственных служащих (PERS).
- Credit Suisse.
- Senateur Investment Group, американский хедж-фонд.
- Jefferies Financial Group Inc., инвестиционная американская компания.
- Birch Grove Capital, американский хедж-фонд.

Ранее известные номинальные частные акционеры-инвесторы:
- Омри Лави (Omri Lavie) 9%.
- Эдди Шалев (Eddy Shalev) 1,8%.
- Шалев Хулио (Shalev Hulio) 9%.
- Алексей Вороновицкий (Alexei Voronovitsky) 0,1% инженер програмист NSO Group.
- Роберт Симондс (Robert Simonds) американский кинопродюсер.
- Эран Горев (Eran Gorev) 0,8% партнер в частной инвестиционной фирмы Francisco Partners.
- Нив Карми(Niv Karmi).
- Кевин Вильсон (Kevin Wilson).
- Стефен Пил (Stephen Peel) бывший партнер в ex-Texas Pacific Group.
- Стефен Ковски (Stefan Kowski) бывший старший руководитель в Centerbridge Partners.
- Бастьян Люкен (Bastian Lueken) возглавлял европейский инвестиционный бизнес в Platinum Equity.

А также:
- Global Seven Group LP 12%.
- ESOP Management and Trust 2,8%.
- Francisco Partners 64,5%.

(Подробнее - см. Приложение 1).

Изначально в 2010 году NSO Group финансировалась группой инвесторов под руководством израильтянина Эдди Шалева (Eddy Shalev), партнера-основателя инвестиционного фонда Genesis Partners, в размере 1,8 миллиона долларов (30% акций компании) и Джошуа Лашер (Joshua Lasher).

2 декабря 2013 года основатели Group NSO создали и зарегистрировали еще одну компанию в Израиле под названием L.E.G.D. Company Ltd.

С 19 марта 2014 L.E.G.D. Company Ltd. стала крупнейшим акционером и управляющим директором NSO Group Technologies Ltd.

Francisco Partners OSY - L.E.G.D

Первая ступень в финансовой пирамиде Francisco Partners OSY - L.E.G.D.
В 2014 году американская Francisco Partners, одна из ведущих мировых инвестиционных фирм, специализирующаяся на партнерстве с высоко технологическими ориентированными компаниями, выкупила Group NSO за 120 миллионов долларов. Также Francisco Partners прирастила к Group NSO филиал под названием Circles (компания специализируется на исследованиях уязвимости телекоммуникационных инфраструктур, основана в 2008 году и тоже приобретенная в 2014 году Francisco Partners).

Для справки: Структурирование сделки приобретения Francisco Partners NSO Group Technologies Ltd. включало:

- создание фондом Francisco Partners OSY Holdings Ltd. на Каймановых островах в начале 2014 года;
- создание в феврале 2014 года компанией OSY Holdings Ltd. OSY Technologies SARL в Люксембурге;
- OSY Technologies SARL становится единственным акционером израильской компании L.E.G.D. Company, которая на момент приобретения была крупнейшим акционером NSO Group Technologies Ltd;
- Фонд инвестиций Francisco Partners таким образом стал конечным крупным акционером NSO Group Technologies Ltd.

Francisco Partners Square 2 SARL - Triangle Holdings SA

Вторая ступень в финансовой пирамиде Francisco Partners Square 2 SARL - Triangle Holdings SA.

В конце ноября и начале декабря 2014 года было создано два дополнительных уровня холдинговых компаний в цепочке собственности между OSY Holdings Ltd. и OSY Technologies SARL, при этом лица, связанные с NSO Group Technologies Ltd., на этот раз приобрели доли в собственности самих холдинговых компаний, а следовательно, и в полном комплексе дочерних операционных компаний под управлением OSY Technologies.

Новые компании следовали тому же шаблону финансовой архитектуры, присутствующему в других частях корпоративной структуры:

- Square 2 SARL и Triangle Holdings SA были зарегистрированы в Люксембурге 21 ноября 2014 года.
- На момент регистрации OSY Holdings Ltd. стала единственным акционером Triangle Holdings SA,

- Triangle Holdings SA, в свою очередь, стала единственным акционером Square 2 SARL.
- Square 2 получила полное владение OSY Technologies SARL после передачи акций от OSY Holdings Ltd.

OSY Holdings Ltd., принял решение о расширении владения Triangle Holdings SA путем выделения определенного количества акций Triangle Holdings SA пятерым физическим лицам и двум компаниям следующим образом:

- Омри Лави, соучредитель NSO (9%).
- Шалев Холи (Хулио), соучредитель NSO (9%).
- Эдди Шалев, первоначальный инвестор NSO (1,8%).
- Алексей Вороновицкий, бывший инженер-программист в Израильских оборонных силах (0,1%).
- Эран Горев, партнер операционного управления Francisco Partners и председатель NSO Group (0,8%).
- ESOP Management and Trust Services Ltd. израильская компания (2,8%) компанией.
- Global Seven Group LP зарегистирирована на Британских Виргинских островах (12%).
- ESOP, Омри Лави, Шалев Хулио, Эдди Шалев и Алексей Вороновицкий использовали акции NSO Group Technologies Ltd. в качестве вклада в натуре для оплаты новых акций Triangle Holdings SA.

Triangle Holdings SA оказался в собственности:

- новых 5 акционеров 35,5%.
- OSY Holdings Ltd. (Francisco Partners), 64,5%.

В 2015 году Francisco Partners пытался продать Group NSO, но безуспешно, из-за имиджевых проблем, связанных со своей клиентурой.

29 мая 2016 года наименование крупнейшего акционера NSO Group Technologies Ltd. L.E.G.D. Company Ltd. официально было изменено на Q Cyber Technologies Ltd. принадлежащую OSY Technologies SARL.

В июне 2017 года NSO Group Technologies Ltd. снова выставлена на продажу за сумму более 1 миллиарда долларов (в десять раз больше, чем при покупке в 2014).

В июле 2017 срывается сделка о продаже американской компании Verint Systems. Blackstone Group также вел переговоры о покупке части NSO, безрезультатно.

14 февраля 2019 года Francisco Partners реализует продажу 60% Group NSO частному европейскому инвестиционному фонду Novalpina Capital (Novalpina Capital Partners I SCSp), с штаб-квартирой в Лондоне и двум соучредителям Group NSO Шалеву Хулио и Омри Лави. Сделка реализована через люксембургскую компанию Novalpina Capital

Partners I LuxCo SARL, которая использует свою люксембургскую компанию NorthPole Holdco SARL.

Novalpina Capital Square 2 SARL - NortPole

Третья ступень в финансовой пирамиде Novalpina Capital Square 2 SARL – NortPole.
В 2019 году, снова по шаблону, люксембургская компания Square 2 SARL, которая полностью принадлежала Triangle Holdings SA и служила единственным акционером OSY Technologies SARL, была использована для объединения инвесторских лагерей Novalpina и NSO.

Дополнительные структурные изменения изменили баланс Square 2 SARL в OSY Technologies SARL (которая, как отмечалось ранее, является материнской компанией нескольких операционных сущностей NSO).
В апреле 2019 года в результате этих транзакций:

- Triangle Holdings SA, по-прежнему владел оригинальными акциями Square 2 SARL (31,4%).
- NorthPole Holdco SARL, новый акционер, владел вновь выпущенными акциями Square 2 SARL (68,6%).
- Square 2 SARL стал прямым и 100% владельцем NorthPole Bidco SARL, которая владеет на 100% NorthPole Newco SARL, которая владеет на 100% OSY Technologies SARL. OSY Technologies SARL продолжает владеть операционными сущностями IOTA Holdings Ltd., Q Cyber Technologies SARL, Q Cyber Technologies Ltd. и Westbridge Technologies Inc., а также их дочерними компаниями.

Novalpina Capital Emerald LIE SARL - Diamond LIE SARL

Четвертая ступень в финансовой пирамиде Novalpina Capital Emerald LIE SARL - Diamond LIE SARL.

7 февраля 2020, опять по шаблону, был добавлен еще один уровень новых корпоративных сущностей:

- было создано частное акционерное общество Emerald LIE SARL.
- NorthPole Bidco SARL выступило в качестве единственного акционера Emerald LIE SARL.
- В тот же день Emerald LIE стала единственным акционером вновь созданной люксембургской компании Diamond LIE SARL.

В результате Emerald LIE и Diamond LIE были интегрированы непосредственно в сеть холдингов NSO Group Technologies, а именно между NorthPole Bidco SARL и NorthPole

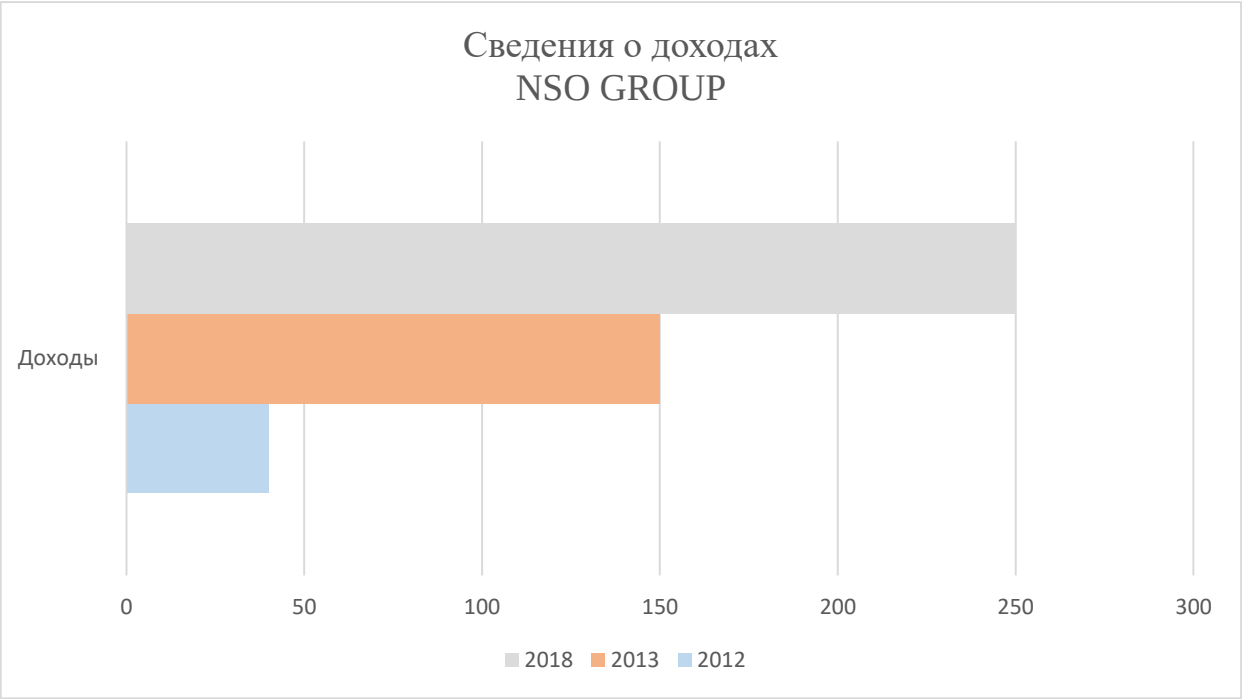
Newco SARL и компании Goatilev, приобретенных ранее NorthPole Bidco SARL, теперь находятся в совладении с NorthPole Newco SARL.

В июле 2021 года, после разногласий, инвесторы Novalpina Capital (а именно группа NOAL SCSP: Oregon Public Employee Retirement Fund (OPERF), CNP Assurances, The Centrica Combined Common Investment Fund) лишили фонд контроля над своими активами. Контроль был передан консалтинговой фирме Berkeley Research Group (Berkeley Asset Management) с штаб-квартирой в Калифорнии, включая NSO Group.

В 2022 году L3Harris Technologies, американская военная компания с опытом в секторе разведывательной технологии, вела переговоры о возможности приобретения NSO Group, без конкретизации какой-либо сделки.

В марте 2023 года Омри Лави, после судебных схваток между NSO Group и TREO Asset Management (ex-BRG Asset Management) завладел контрольным пакетом акций через свою люксембургскую компанию Dufresne Holdings, которой были переданы акции NorthPole, материнской компании NSO Group Technologies Ltd.

Сведения о доходах



- 2013 г. - годовой доход NSO Group составил около 40 миллионов долларов США.
- 2014 г. - после покупки американской частной инвестиционной компанией Francisco Partners выручка NSO Group за этот год в явном виде не указана.
- 2015 г. - годовой доход компании значительно вырос и составил около 150 миллионов долларов.

- 2016-2017 г.г. - в открытых источниках отсутствуют конкретные данные о годовой выручке за эти годы.
- 2018 г. - выручка компании составила 250 миллионов долларов, а число лицензированных клиентов - десятки.
- 2019-2020 г.г. - в открытых источниках отсутствуют конкретные данные о годовой выручке за эти годы.
- 2021-2024 г.г. - в предоставленных источниках отсутствуют конкретные данные о выручке за эти годы.

Для примера: за период 2012-2018 гг. федеральное правительство Мексики потратило на Pegasus до 300 миллионов долларов, часть из которых по откатной схеме осело в карманах чиновников, военных и правоохранителей.

Сведения о финансировании деятельности и сделках с активами компании

На протяжении многих лет финансирование NSO Group поступало из различных источников. Первоначально компания финансировалась ее основателями и ранними инвесторами. Позже она привлекла значительные инвестиции от частных инвестиционных компаний.

В 2019 году лондонская фирма Novalpina Capital заключила сделку по покупке контрольного пакета акций NSO Group вместе с основателями компании. Стоимость этого приобретения составила около 1 миллиарда долларов. До этого американский фонд прямых инвестиций Francisco Partners принял решение продать NSO Group этой новой группе инвесторов.

Однако между соучредителями Novalpina Capital возникли внутренние разногласия, которые привели к переговорам о передаче управления фондом, которому принадлежит NSO Group, американской консалтинговой фирме Berkeley Research Group.

В 2023 году стало известно, что Омри Лави получил контроль над компанией после многочисленных судебных тяжб между NSO и американской финансовой фирмой Treo, которая ранее контролировала фонд прямых инвестиций, владевший контрольным пакетом акций NSO Group.

Таким образом, каналы финансирования NSO Group включают прямые инвестиции в акционерный капитал, внутреннее финансирование от ее учредителей и, возможно, управление собственным фондом консалтинговой фирмой. Компания также инвестировала в лоббистские усилия по формированию своей бизнес-среды в Соединенных Штатах.

Одним из основных результатов финансирования деятельности NSO Group является разработка и сопровождение ее технологий. NSO Group известна своими сложными инструментами кибербезопасности, такими как ПО Pegasus. Разработка таких передовых технологий требует значительных ресурсов, включая высококвалифицированный персонал, современное оборудование и обширные исследования и разработки. Финансирование обеспечивает необходимые ресурсы для этой деятельности, позволяя NSO Group сохранять свои позиции ведущего игрока в индустрии кибербезопасности.

Финансирование также позволяет NSO Group расширять свой бизнес. Например, приобретение Novalpina Capital и основателями компании контрольного пакета акций NSO Group в 2019 году стоимостью около 1 миллиарда долларов, вероятно, предоставило компании дополнительные ресурсы для расширения своей деятельности и выхода на новые рынки.

Кроме того, финансирование играет решающую роль в способности NSO Group справляться с проблемами регулирования. Компания столкнулась с серьезными проблемами контроля и регулирования в различных юрисдикциях из-за противоречивого характера своих технологий. Финансирование позволяет NSO Group участвовать в лоббистских усилиях и судебных баталиях для решения этих проблем. Например, в 2022 году NSO Group потратила более 1,1 миллиона долларов на компании по связям с общественностью и юридические фирмы в США в рамках своей кампании по отмене включения Министерством торговли США в список компаний, деятельность которых ограничена в торговле.

Таким образом, финансирование оказывает значительное влияние на деятельность NSO Group, позволяя компании разрабатывать и поддерживать свои технологии, расширять свой бизнес и решать проблемы регулирования. Например, NSO Group приобрела компанию Circles, что стало стратегическим шагом по укреплению ее технологических возможностей и расширению ассортимента продукции.

Коммерческие заказчики организации

Основным, но не единственным продуктом NSO Group является разведывательное ПО Pegasus. Это программное обеспечение, предназначенное для атак на смартфоны с операционными системами iOS и Android, коммерциализируется с 2013 года. Pegasus составляет 75% продаж.

В начале 2024 года NSO Group официально насчитывала 56 клиента в 31 стране. Список коммерческих государственных клиентов не разглашается.

Из них 46% клиентов - органы полиции, 45% - разведывательные агентства, а 9% - вооруженные силы.

У компании есть список из 58 стран, известных как «D-страны», с которыми компания не ведет бизнес. Этот список проходит ежегодное обновление и обзор Менеджмент-комитетом.

Способ отбора клиентов

В настоящий момент при оценке страны-клиента используются девять признанных индексов управления и прав человека.

Среди источников:

- Мировой банк;
- Демократический индекс The Economist;
- Индекс хрупких государств Фонда мира;
- Свобода в мире от Freedom House;
- Свобода интернета от Freedom House;
- Индекс свободы прессы без границ;
- Индекс восприятия коррупции Transparency International;
- Глобальный индекс мира;
- Индекс гражданского общества CIVICUS;

- Матрица риска взяточничества TRACE International.

Эти данные генерируют «Оценку страны» от 1 до 100. Также оценивается риски, связанные с каждой потенциальной бизнес-возможностью, и присваивает "Категорию возможности" A, B, C или D. При этом учитываются:

- тип продукта для продажи;
- географические границы, в пределах которых может быть выпущен продукт;
- тип организации клиента и определенная миссия;
- срок действия предполагаемого лицензионного соглашения;
- применимые законы и регламенты по экспортному контролю, включая эмбарго и санкции;
- членство клиента в международных организациях и статус по отношению к основным международным договорам или конвенциям, касающимся прав человека.

NSO Group не продает свою продукцию в страны под санкциями, в страны, находящиеся в черном списке Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ), в страны, в которых нарушаются права человека согласно вышеперечисленным источникам.

Доверенные клиенты

Первостепенные, с высоким уровнем доверия и общими стратегическими интересами являются страны разведывательного альянса Пять глаз (англ. Five Eyes). В альянс входят Австралия, Канада, Новая Зеландия, Великобритания и США. Эти страны являются участниками многостороннего договора о совместном сотрудничестве в области радиоэлектронной разведки. Второй уровень включает страны НАТО, многие из них уже являются клиентами:

1. Англия Five Eyes
2. Албания (2009)
3. Австралия Five Eyes
4. Бельгия (1949)
5. Болгария (2004)
6. Венгрия (1999)
7. Германия (1955)
8. Греция (1952)
9. Дания (1949)
10. Исландия (1949)
11. Испания (1982)
12. Италия (1949)
13. Канада (1949) Five Eyes
14. Латвия (2004)
15. Литва (2004)

16. Люксембург (1949)
17. Нидерланды (1949)
18. Новая Зеландия Five Eyes
19. Норвегия (1949)
20. Польша (1999)
21. Португалия (1949)
22. Румыния (2004)
23. Северная Македония (2020)
24. Словакия (2004)
25. Словения (2004)
26. США (1949) Five Eyes
27. Турция (1952)
28. Финляндия (2023)
29. Франция (1949)
30. Хорватия (2009)
31. Черногория (2017)
32. Чехия (1999)
33. Швеция (2024)
34. Эстония (2004)

Анализ медиа- данных, опирающихся на многочисленные журналистские расследования, указывает, что в разные периоды клиенты NSO Group были локализированы в следующих странах:

- Азербайджан
- Алжир
- Бангладеш
- Бахрейн
- Бельгия
- Болгария
- Венгрия
- Гана
- Германия
- Дания
- Египет
- Израиль
- Индия
- Индонезия
- Иордания
- Испания
- Испания
- Казахстан
- Кения

- Латвия
- Люксембург
- Мальта
- Марокко
- Мексика
- Нидерланды
- Объединенные Арабские Эмираты
- Панама
- Польша
- Руанда
- Сальвадор
- Саудовская Аравия
- Сербия
- Сербия
- США
- США Для Джибути
- Таиланд
- Того
- Уганда
- Узбекистан
- Финляндия
- Эстония

По данным журналистских расследований (2021, Amnesty International, Citizen Lab, Forbidden Stories), выявлены 45 стран с подозрением на разведывательное программное обеспечением Pegasus (см. Приложение 1). Важно отметить, что атаки могут осуществляться на номера телефонов с чужих территорий.

Проекты для госведомств и спецслужб

Самым известным продуктом компании является программное обеспечение Пегас («Pegasus»). Оно было впервые использовано израильской полицией в 2013 году, после того как к этим ПО воспользовались командиры подразделений Шабак и военной разведки. «Эти новые разоблачения - всего лишь естественный процесс искалеченной и подорванной демократии Израиля, которая контролируется мощным аппаратом военной безопасности», - предупредил Йосси Меллман, эксперт-аналитик, на страницах Haaretz. Расследования, проведенные Генеральной прокуратурой, которая

рассчитывала именно на техническую помощь Шабака и Моссада, в итоге сняли с израильской полиции обвинения в незаконном прослушивании телефонных разговоров.

Pegasus, разработанный NSO, полностью отличается от подобного программного обеспечения. Он устанавливается на мобильный телефон заочно, без необходимости пользователю выполнять какие-либо операции, и действует без его ведома. Когда владелец устройства понимает, что за ним следят, Pegasus уже извлек всю информацию и данные.

Эксперты говорят, что программа настолько полная и сложная, что она знает обо всех нас больше, чем мы сами: о передвижении, обмене сообщениями, об установленных приложениях.

Кроме того, когда вы запускаете антивирус, Pegasus не обнаруживается и автоматически гаснет, не оставляя следов, и пользователь не узнает, что ПО было на устройстве. Pegasus может запускать рекордер и включать съемочную камеру по умолчанию, даже если мобильный телефон выключен.

Поэтому, когда пользователь выключает устройство и воображает, что оно отключено, любая спутниковая программа-локатор все время точно знает, где находится человек.

Pegasus рассматривается в Израиле как «кибероружие, которое допускает спонсируемый государством терроризм против гражданского общества».

Компания NSO постоянно пропагандирует свое ПО: «Эта программа является кибер-разведкой для глобальной безопасности и стабильности. NSO создает технологии,

чтобы помочь правительственным учреждениям предотвращать и пресекать терроризм и преступления, которые могут спасти тысячи жизней». Таким образом, вопреки рекламе компании, которая говорит о Pegasus как о чем-то хорошем и выгодном, что правительства могут приобрести для борьбы с терроризмом и спасения жизней, на деле это ПО широко используется в политических целях.

45% реализованных NSO Group правительствам различных стран ПО приходится на разведывательные управления, 46% - на правоохранительные органы и 9% - на подразделения министерства обороны.

Мексика

Первым клиентом NSO Group стало правительство Мексики, ведущее борьбу с наркокартелями, на тот момент искавшее способы взломать зашифрованную службу обмена сообщениями BlackBerry, которую предпочитают боевики картеля. АНБ нашло способ проникнуть внутрь, но американское агентство предлагало Мексике лишь спорадический доступ.

После этого мексиканцы воспользовались услугами израильской компании. По данным средств массовой информации, правительство Мексики заплатило 15 миллионов долларов за оборудование и ПО и ещё 77 миллионов — за слежку за членами наркокартеля. По мнению мексиканских чиновников, Pegasus сыграл важную роль в поимке наркобарона Эль Чапо, которого приговорили к пожизненному заключению в феврале 2019 года.

Правительство Мексики также использовало хакерские инструменты для слежки за оппозиционерами, журналистами, международными следователями, которые расследовали нераскрытое исчезновение 43 студентов, признанных мёртвыми, и даже за сторонниками налога на газированную воду. Жертвы получали контекстные сообщения, например, о смерти родственников, со ссылками, переход по которым взламывал телефоны.

Саудовская Аравия

В конце 2018 года активист Омар Абдул Азис из Саудовской Аравии подал в суд на NSO Group, утверждая, что компания взломала телефон его друга, журналиста Джамаля Хашогджи, убитого 2 октября 2018 года в Стамбуле.

По данным средств массовой информации, NSO Group с 2017 года помогала в слежке за журналистами и активистами в Саудовской Аравии бывшему принцу Сауду аль-Кахтани, которого подозревали в причастности к убийству Хашогджи.

В переписке с NSO Group аль-Кахтани отмечал, что собирается использовать инструменты компании для слежки «на всём Ближнем Востоке и в Европе» — Франции, Турции, Катаре и Великобритании.

ОАЭ

ПО Pegasus использовалось для слежки за оппозиционерами, в частности, за Ahmed Mansoor, которого неудачно попытались взломать, подослав на его iPhone вредоносную ссылку в текстовом сообщении. Именно исследование этой ссылки специалистами Citizen Lab позволило получить первые технические данные о функционировании Pegasus.

Индия

Впервые использование Pegasus было зафиксировано исследователями Citizen Lab в 2018 году при идентификации ряда операторов ПО, один из которых, Ганг (Ganges), был активен в первую очередь в интернет-сетях Индии.

В 2019 году атаке подверглись 121 человек, среди которых журналисты, активисты, юристы-правозащитники. Подозрение пало на правительство премьер-министра Нарендра Моди; оппозиционеры в индийском парламенте потребовали расследовать инцидент на уровне Верховного суда.

Пакистан

В 2019 году было заявлено о слежке неизвестными лица за несколькими десятками высокопоставленных пакистанских чиновников, среди которых — представители министерства обороны и разведслужб. В этом случае использовалась уязвимость в WhatsApp.

Панама

Президент Панамы Рикардро Мартинелли (2009-2014) использовал продукт NSO против политических оппонентов, судей, профсоюзных лидеров, деловых конкурентов — все «без соблюдения юридической процедуры». Позже прокуроры заявили, что Мартинелли даже приказал команде, управляющей Pegasus, взломать телефон его любовницы. Все закончилось в 2014 году, когда Мартинелли сменил его вице-президент Хуан Карлос Варела, который сам утверждает, что был объектом разработки Мартинелли. Подчиненные Мартинелли ликвидировали разведывательную систему, и бывший президент бежал из страны.

Азербайджан

В рамках проекта Pegasus, Forbidden Stories впервые смогла задокументировать использование Pegasus в Азербайджане. В качестве целей были выбраны более 40 азербайджанских журналистов, в том числе репортеры Azadliq.info и Mehdar TV, двух из единственных оставшихся независимых СМИ в стране.

В Азербайджане большинство независимых новостных агентств заблокированы, а члены семей журналистов регулярно подвергаются преследованиям со стороны властей. При президенте Ильхаме Алиеве, чья семья правила Азербайджаном на протяжении десятилетий, пространство для критических голосов, по мнению Хьюман Райтс Вотч, «практически уничтожено» (тот же Хьюман Райтс Вотч проводил техническую экспертизу телефонов азербайджанских журналистов дабы установить факт наличия вредоносного ПО).

Другие продукты компании

Kaymera

Шалев Хулио и Омри Лави также являются сооснователями компании Kaymera, которая занимается кибербезопасностью. Она обещает клиентам «комплексный многоуровневый подход к защите мобильных устройств». Kaymera запустили в 2014 году, фирма привлекла 3 миллиона долларов от частных инвесторов.

«Любой, кто видит возможности NSO Group, сразу же думает о том, как защититься от подобных инструментов. Мы решили создать компанию, когда увидели в этом потенциал», — рассказал глава компании Ави Розен в телефонном разговоре с Bloomberg в 2014 году. Он подтвердил, что сотрудничал с Лави и Хулио, но они не участвуют в операционной деятельности компании и NSO работает отдельно.

Таким образом, в кибервойнах NSO и Kaymera помогают противоборствующим сторонам: одна компания продаёт правительству инструменты для разведывательной деятельности, другая — продукты для защиты от этой же технологии, считает Bloomberg.

Convexum

Основана в 2015 году бывшими членами известного подразделения разведки 8200 ЦАХАЛа, базируется в Тель-Авиве, занимается разработкой способов перехвата и защиты от дронов путем контроля канала связи между планером и оператором, в феврале 2020 года была приобретена NSO-Group за 60 миллионов долларов.

Convexum использует методы кибербезопасности для устранения угроз дронов в радиусе 1,5 км. Как только подозрительный дрон обнаружен с помощью радиочастотных датчиков, технология, называемая манипуляцией протоколом (спуфинг), позволяет захватить БПЛА автоматически или вручную. Convexum утверждает, что является единственным решением на рынке, которое может обнаружить не авторизованный дрон, выпущенный в пределах защищенного периметра. Система не создаёт помехи для беспроводной связи и GPS, успешно работает в плотной городской застройке.

Circles

Наступательная киберкомпания Circles Technologies имеет тесные деловые связи с NSO Group, и, согласно многочисленным отчетам, даже находится под ее контролем или под контролем основателей NSO Group. Согласно утечки финансовых документов с Кипра «Секреты Кипра», были выявлены свидетельства того, что компания была приобретена NSO Group в 2014 году через зарегистрированную в Люксембурге дочернюю компанию. Circles Technologies зарегистрирована на Кипре и работает из Болгарии. Основана двумя израильтянами Боазом Гольдманом и Талом Диляном в 2011 году. Факт регистрации компании на Кипре, позволяет, обходить экспортные ограничения Израиля.

Circles Technologies специализируется на мониторинге и наблюдению в сетях сотовой связи, а именно, используя слабые места в сетях мобильных телефонов, чтобы получать сведения о звонках, СМС и информацией о местоположении.

Circles Technologies была независимым поставщиком разведывательных агентств до 2014 года, когда была приобретена частной акционерной компанией Francisco Partners за 130 миллионов долларов и слилась в более крупную компанию по слежке. В эту зонтичную организацию также входила израильская компания NSO Group, которая разработала Pegasus.

Технология Snooping, используемая Circles Technologies, известна как эксплуатация уязвимостей Signaling System 7 (SS7), мощного, но трудного для обнаружения инструмента в правительственных разведывательных арсеналах.

Многие из стран, перечисленных как вероятные клиенты Circles Technologies, имеют опыт использования инструментов наблюдения против диссидентов и активистов.

В иске против Circles Technologies, поданном в 2018 году израильскими адвокатами Алаа Махаджной и Мухаммадом Далехом, приведен пример как минимум одного случая, когда менеджер Circles Technologies пытался продать разведывательные программы компании высокопоставленным членам правительства ОАЭ, взломал четыре запрошенных телефона и отправил данные клиенту.

Израиль является одной из стран, перечисленных в качестве клиентов Circles в отчете Citizen Lab. По данным Citizen Lab, система использовалась Израилем, по крайней мере, в какой-то момент, но подробности об этом использовании ограничены.

Другими компаниями, которые были основаны и принадлежат Таль Дилиан, основателю Circles Technologies являются:

Cytrox

Компания была основана в 2017 г. Разработала разведывательную технологию «Predator». Имеет клиентов в Греции, Сербии, Германии, Египте, Армении, Саудовской Аравии, Омане, Колумбии, Кот-дИвуаре, Вьетнаме и Филиппинах. Разработки компании, так же использовались с целью наблюдения за деятельностью журналистов.

Справочно:

Таль Дилиан – полковник по резервам в Армии Израиля, служил в качестве главного командира Технологического подразделения армии, на нескольких должностях в штабе Разведывательного корпуса. Таль Диллиан также является основателем и владельцем других компаний по кибервразведке и наблюдению, таких как Intellexa, Cytrox (которая разработала «Хищника») и WiSpear (переименована в Passitora).

Intellexa

Предлагает технологии, которые предназначены для правоохранительных органов и спецслужб, чтобы «помочь защитить население». **Intellexa** разрабатывает и продает средства слежки и вредоносные программы, предназначенные для международных правоохранительных органов. Штаб-квартира в Греции.

WiSpear – основана в 2016 году. Разрабатывает технологию перехвата Wi-Fi и крадет данные.

Bold

В феврале 2023 года было опубликовано, что 22 из 26 сотрудников новой израильской компании кибервразведки Bold являются бывшими сотрудниками NSO Group. Также президент и вице-президенты Bold были бывшими старшими директорами NSO.

Fleming

В марте 2020 года, с ростом COVID-19, NSO Group запустил технологию отслеживания контактов под названием «Fleming». Программное обеспечение предназначено для отслеживания и картирования распространения COVID-19 с использованием геолокационных данных с мобильных телефонов, в том числе с помощью данных, собранных внешними сторонними приложениями. Затем системы предоставляют информацию о контактах и длительности инфицированных людей, которые могут быть индивидуально отслежены, создают карты «heat» для выявления горячих точек распространения вируса, и предоставить анализ риска того, насколько вероятно, что каждый человек или группа населения будут заражены вирусом.

Израильский министр обороны в то время Нафтали Беннет был восторженным сторонником разработки и использования программного обеспечения в Израиле. Система использовалась в рамках контактного отслеживания израильтянами израильской службы безопасности в течение всего 2020 года.

В марте 2020 года по информации полученной из СМИ стало известно, что «Fleming» может анализировать огромные объемы данных для отображения движений людей. Инструмент отслеживает граждан, присваивая им случайные идентификаторы, которые правительство может деанонимизировать в любой момент.

Отчет Forensic Architecture, опубликованный в декабре 2020 года, сообщал о базе данных, собранной программой «Fleming» NSO Group, которая оказалась незащищенной в сети Интернет. Она содержала более пяти сотен тысяч данных для приблизительно 32 000 различных мобильных телефонов. Эта база данных использовалась в качестве маркетингового инструмента для продвижения системы на рынке стран по всему миру. Отслеживаемые мобильные телефоны принадлежали гражданам Израиля, ОАЭ, Бахрейна, Саудовской Аравии и Руанды — все это страны с контрактными отношениями с NSO Group.

Phantom

Во время презентации для официальных лиц в Вашингтоне компания продемонстрировала новую систему, названную «Phantom», которая может взломать любой номер в Соединенных Штатах, на который FBI укажет. Израиль предоставил NSO Group специальную лицензию, которая позволила его системе «Phantom» атаковать номера США. Лицензия разрешала только одному типу клиентов: государственным учреждениям США.

Простая брошюра, составленная для потенциальных клиентов дочерней компанией NSO Group в США, говорит, что «Phantom» позволяет американским

правоохранительным органам и разведывательным агентствам получать информацию «путем извлечения и мониторинга важных данных с мобильных устройств.» Это независимое решение, которое не требует сотрудничества со стороны AT & T, Verizon, Apple или Google. Система, по ее словам, превратит смартфон вашей цели в интеллектуальный золотой рудник.

Dream Security

Шалев Хулио основал компанию Dream Security совместно с Себастьяном Курцем для обеспечения кибербезопасности критически важных инфраструктурных объектов.

Также партнёрами NSO являются:

- **Израильская компания Ability Inc.**

  Ее технология неограниченного перехваата (ULIN) позволяет перехватывать голосовые вызовы, SMS-сообщения и информацию, связанную с вызовами телефонов GSM/UMTS/LTE, без необходимости находиться рядом с перехватываемым телефоном и без согласия операторов мобильной связи, и требует только номера телефона мобильного устройства или IMSI. Служба «Ability» использует слабое место в SS7, системе сигнализации № 7.

  Являясь основной частью мировой сетевой инфраструктуры, SS7 помогает маршрутизировать вызовы между различными операторами связи и центрами коммутации. Поставщики услуг часто используют SS7 для поддержки связи в регионах, где обычная сеть клиента недоступна, например, когда пользователь находится за границей. (Владельцы Ability Inc. некто Анатолий Хургин и Александр Ауровский).

- **Израильская компания Cellebrite,** сотрудничающая с полицией США, отметила что сотрудничает с NSO Group, и, по словам представителя Cellebrite (Leeor Ben Peretz), NSO Group больше вовлечена в мир разведки и следит за целями без их ведома и согласия, в то время как Cellebrite занимается получением доступа к содержимому телефона после того, как их конфисковала полиция. Также Леор упомянул о том, что между компаниями происходит переток кадров (технических специалистов).

- В NSO также работают бывшие сотрудники ряда других известных израильских поставщиков разведывательной информации, включая **Nice Systems** и **Elbit**.

- **Candiru** была основана инженерами, покинувшими NSO Group.

  Последние события кардинально изменили корпоративную структуру компаний NSO Group, некоторые филиалы, работающие над спецпроектами, были проданы.

Так, например, Westbridge Technologies, представительская компания NSO Group, специально созданная для продаж в США, больше не существует. Была замечена при контактах и сделках с FBI - Федеральное бюро расследований (Federal Bureau of Investigation), DEA - Управление по борьбе с наркотиками (Drug Enforcement Administration), CIA - Центральное разведывательное управление. Посредниками при покупке Pegasus выступил Riva Networks Inc. под вымышленным названием Cleopatra Holding.

Предлагается продолжить наблюдение за значимыми проектами, которые велись филиалами и дочерними компаниями:

- **Pegasus**, NSO Group Technologies Ltd.
  Система наблюдения и сбора данных с мобильных устройств конкретных лиц, подозреваемых в участии в террористической или преступной деятельности без авторизации, дистанционно.

- **Eclipse,** система противодействия дронам (компания производитель NSO Group Sentrycs продана в 2022 Berkeley Research Group, инвестором выступил TREO Asset Management). Это платформа, инструмент, который автоматически и автономно обнаруживает, захватывает и безопасно приземляет несанкционированные коммерческие дроны в указанной зоне.

- **Wayout,** система взлома роутеров для операций кибербразведки правоохранительных и разведывательных агентств (сервис (IoT) для государственного использования), по некоторым данным с 2023 года компания Wayout больше не входит в NSO Group.

- **Phantom,** программное обеспечение для взлома шифрования, которое позволяет правоохранительным органам обходить законы о конфиденциальности в США в уголовных делах без сотрудничества с мобильными операторами и такими производителями как Apple или Google.

- **Landmark,** позволяет отслеживать местоположение GPS телефонов.

Деятельность организации в России и странах бывшего СССР

Азербайджан

1000 азербайджанских номеров были в списке проекта Pegasus. Из этого списка пятая часть принадлежала репортерам, редакторам или владельцам медиа компаний. Кроме того, подразумевается, что операция, направленная против посла Франции в Армении, велась с территории Азербайджана с помощью программного обеспечения Pegasus.

Армения

Недавние отчеты показали, что Pegasus использовался во время конфликта между Арменией и Азербайджаном. Телефоны 12 человек, работающих в Армении, включая пресс-секретаря Министерства иностранных дел Армении, официального представителя ООН и нескольких армянских активистов гражданского общества и журналистов (большинство из которых освещали конфликт), предположительно были заражены Pegasus между октябрем 2020 и декабрем 2022 года. Нет доказательств того, что Армения когда-либо была пользователем Pegasus. CitizenLab выявил подозреваемого оператора Pegasus в Азербайджане, который мог осуществлять атаки на цели в Армении.

Согласно отчету CitizenLab, поддерживаемые правительством Армении структуры приобрели Predator, продукт конкурирующего с Pegasus, компании Cytrox.

Казахстан

В Казахстане в 2017 и 2018 годах Бакытжан Сагинтаев, в тот период времени премьер-министр Казахстана, Касым-Жомарт Токаев, который в 2019 году сменил Нурсултана Назарбаева на посту президента страны, и Аскар Мамин, который впоследствии стал премьер-министром, были включены в список потенциальных целей Pegasus, вероятно, самим казахским режимом.

Эстония

В 2018 году Эстония проявила интерес к покупке разведывательного программного обеспечения Pegasus от компании NSO Group. Имели место начальные переговоры

между Эстонией и NSO Group, после чего Эстония внесла предоплату по сделке на сумму 30 миллионов долларов США за программное обеспечение для наблюдения.

Россия

По некоторым данным были попытки установления на российские телефоны Pegasus со стороны Эстонии. Украина же была замечена в попытках приобрести программное обеспечения для установления на российских номерах.

Литва

Литовская компания UAB «Технологии связи», работающая в области «связи и телекоммуникационных услуг», принадлежит Анатолию Хургину, российско-израильскому гражданину, бывшему инженеру израильской армии и соавтору разработки Pegasus вместе с NSO Group. Он является основателем компании Ability Ltd., которая сотрудничала с NSO Group по программе Pegasus и обрабатывала сетевую часть операций NSO Group. Не исключено поэтому, что Pegasus использовался и на территории Литвы.

Украина

По некоторым данным, после того как, Крым в 2014 году был присоединен к Российский Федерации, Украина пыталась связаться с израильским правительством, однако безрезультатно. С 2019 года по август 2022 года, по данным СМИ несколько раз запрашивался доступ к программному обеспечению Pegasus, и официально считается, что Агентство по контролю за оборонным экспортом Израиля заблокировало попытку Украины приобрести ПО Pegasus, опасаясь того факта, что российские власти могут с тревогой и беспокойством воспринять такие действия. Также стало известно, что Михаил Федоров, заместитель премьер-министра Украины по вопросам цифровых технологий, отказался подтвердить информацию о приобретении Pegasus, но признал тот факт, что страна в поисках израильских технологий.

Болгария

До сих пор болгарские власти отрицают предоставление лицензий на экспорт NSO Group или его дочерних компаний. Тем не менее, бывший частный акционер NSO Group, Novalpina Capital подчеркнул, что продукция NSO Group экспортируется из ЕС как из Кипра, так и из Болгарии. Более того, по данным СМИ, некоторые серверы инфраструктуры сети, по которой проводились атаки Pegasus, находятся в болгарском

дата-центре, принадлежащем болгарской компании, в свою очередь принадлежащей NSO Group. В феврале 2022 года Софийская городская прокуратура начала расследование, чтобы установить, использовали ли государственные службы Pegasus незаконно против болгарских граждан.

Узбекистан

По некоторым данным, продукция NSO Group была продана полиции Узбекистана через аффилированную CS-Circles Solutions Ltd., базирующуюся на Кипре.

В сентябре 2021 года Forensic News опубликовала отчеты о поставках, свидетельствующие о том, что в 2020 году Circles поставила оборудование Службе государственной безопасности Узбекистана (СГБ).

Дополнительная информация

Расследования и санкции на государственном политическом уровне (неполный список):

2021

Департамент торговли США поместил компанию в черный список после того, как было установлено, что израильский производитель разведывательного ПО Pegasus действовал «вопреки внешней политике и национальным интересам США», что закрывает выход на североамериканский рынок и серьезно мешает продвижению на мировом рынке продукции NSO Group.

2023

Расследования комиссией Европарламента (PEGA), использования ПО Pegasus и аналогичного разведывательного программного обеспечения - реакция на раскрытие проекта Pegasus в 2021 году.

2024, февраль

В феврале Парламентская комиссия Польши начала свою работу по расследованию скандала вокруг разведывательного ПО Pegasus, а также других средств наблюдения. Многие считают этот случай самым крупным политическим скандалом в Польше с падения коммунизма, символизирующим авторитарное отклонение консервативной партии «Право и справедливость» (PiS), находившейся у власти с 2015 по 2023 год. Использование разведывательного программного обеспечения Pegasus, мощного инструмента для вторжения в смартфоны, разведывательными службами партии бывшего премьер-министра Ярослава Качиньского станет основой парламентской комиссии по расследованию, начавшей слушания 19 февраля 2024. Среди первых вызванных свидетелей - сам Качиньский, бывший премьер-министр Беата Шидло, а также бывшие министры юстиции и внутренних дел Збигнев Зиобро и Мариуш Каминский.

2024

В апреле Испанский Верховный суд возобновил расследование использования программного обеспечения Pegasus израильской кибер-разведывательной фирмы NSO Group для осуществления разведывательной деятельности за премьер-министром Педро Санчесом и другими испанскими политиками.

Судебные иски, связанные с ПО Pegasus (список наиболее громких дел):

2021-2024

Apple Inc. подал иск против ответчиков NSO Group Technologies Limited и Q Cyber Technologies Limited, которые создали и распространяют Pegasus, который, как утверждается, является вредоносным программным обеспечением. NSO Group обвиняется в нарушении Закона о компьютерных мошенничествах и злоупотреблениях и Закона Калифорнийского штата о Недобросовестной Конкуренции.

2019-2024

Meta & WhatsApp подали коллективный иск против NSO Group. NSO Group обвиняется, в том, что с помощью вредоносных голосовых вызовов, предназначенных для заражения целевых телефонов вредоносным ПО и кражи сообщений, получили доступ к 1400 пользователям Meta & WhatsApp, включая по меньшей мере 100 представителей "гражданского общества", таких как журналисты и правозащитники, несмотря на сквозное шифрование WhatsApp.

2022

В апреле Федерация международных прав человека (ФМПЧ), Лига прав человека (ЛПЧ) и Салах Хаммури подали совместный иск во Франции против израильской компании NSO Group Technologies за незаконное вторжение в телефон франко-палестинского защитника прав человека Салаха Хаммури.

2022

Журналисты El Faro из Сальвадора подали в США иск в калифорнийский суд через Фонд Найт, организацию защиты прав человека, против NSO Group. Заявители считают, что NSO Group нарушила американский закон, поскольку ее программное обеспечение было использовано для незаконного доступа к данным, хранящимся на серверах Apple в Калифорнии; кроме того, один из сотрудников El Faro, чей телефон был заражен, является гражданином США.

Судебные иски во внутренних конфликтах (список наиболее громких дел):

Многочисленные споры среди акционеров раскрывают разделение внутри группы NSO Group, где некоторые компании сосредотачиваются на разработке защитных киберпродуктов, а другие на атакующих киберпродуктах. Будучи связанными финансово и административно, все несут серьезные издержки из-за скандалов вокруг Pegagsus, конфликта с Департаментом по торговле США, информационной медиа войны, развязанной конкурентами.

2021

Конфликт между менеджерами Novalpina Capital. Адвокат Стефена Пила (Stephen Peel) - против совета директоров и Стефен Ковски (Stefan Kowski), Бастьян Люкен (Bastian Lueken).

2022

Судебные разбирательства между акционером NSO Group, Berkeley Research Group (BRG), NSO Group и Novalpina.

Общественные движения и расследования против NSO Group (список наиболее громких дел)

2015-2016
Дэвид Кей, специальный докладчик ООН по вопросам свободы мнений и выражений против.

2019
Amnesty International.

2016-2020
Citizen Lab.

2021
Forbidden Stories (расследование 17 медиа организаций в 10 странах, координируемое Forbidden Stories при технической поддержке Лаборатории безопасности Amnesty International).

Конкурирующие компании

Pegagus - не единственный продукт дистанционного наблюдения. Конкурирующая продукция присутствует на мировом рынке, включая другие израильские фирмы и продукты Cellebrite, Candiru, Paragon Solutions, Predator, Cytrox, Cellebrite, QuaDream и Intellexa и др.

Из израильских медиа- источников известно, что конкурирующая компания QuaDream Ltd. была создана бывшими офицерами и сотрудниками NSO Group Technologies Гаем Гева (Guy Geva) и Нимродом Резником (Nimrod Reznik). Предполагается, что Quadream разработала инструменты, аналогичные используемым NSO Group. Среди ее клиентов было правительство Саудовской Аравии и, по крайней мере, 10 стран на континентах Северной Америки и Европы.

Из израильских медиа- источников известно, что Шалев Хулио (Shalev Hulio) покинул NSO Group, чтобы основать Dream Security вместе с бывшим канцлером Австрии Себастьяном Курцем (Sebastian Kurz) и Гилом Долев (Gil Dolev). Компания по кибербезопасности на основе искусственного интеллекта Dream Security, сосредоточена на кибербезопасности инфраструктуры, такой как газопроводы, нефтепроводы и водопроводы, чтобы защитить их от вымогательских программ и террористических атак. Полный список конкурентов см. в Приложении №3.

Судебные разбирательства против NSO Group

Юрисдикция	Дата начала	Статус судебного разбирательства	Судебные разбирательства
США	2023	Продолжается	В 2023 году Ханан Элатр, вдова Джамаля Хашогги, подала иск в Северном округе Вирджинии против NSO Group. Согласно судебному иску, ПО Pegasus от NSO Group использовалось для атаки на Элатр за несколько месяцев до убийства ее мужа. В октябре 2023 года иск был отклонен на основании отсутствия персональной юрисдикции. Элатр обжаловала данное решение.
Таиланд	2022/2023	Продолжается	iLaw готовит судебный иск против правительства Таиланда за предполагаемое нападение на 30 активистов и юристов в 2020-2021 годах с помощью ПО Pegasus. В 2022 году iLaw также подала отдельный гражданский иск против NSO Group в суд Таиланда. Кроме того, в июне 2023 года юрист по правам человека Арнон Нампа и защитник правовой реформы Йингчип Атчанонт подали в суд Таиланда иск против различных государственных учреждений Таиланда, обвиняемых в нарушении конфиденциальности с помощью ПО Pegasus от NSO Group.
Великобритания	2022	Продолжается	Юсуф аль-Джамри, бахрейнский активист, получивший политическое убежище в Великобритании, предпринял предварительные шаги для предъявления иска NSO Group и правительству Бахрейна в судах Великобритании после того, как узнал, что его телефон был заражен Pegasus в августе 2019 года. 6 декабря 2022 года в посольство Бахрейна в Лондоне и в NSO Group были отправлены письма, предшествующие предъявлению претензии.
США	2022	Продолжается	Журналисты и другие лица, которые пишут, производят и издают цифровую газету «El Faro», базирующуюся в Сальвадоре, подали в федеральный суд США на NSO Group и Q Cyber Technologies Limited. В жалобе утверждается, что в период с июня 2020 года по ноябрь 2021 года истцы стали жертвами атак ПО Pegasus, а к их устройствам «осуществлялся удаленный и тайный доступ, их коммуникации и действия отслеживались, а их личные данные были

			доступны и украдены». В марте 2024 года жалоба была отклонена.
Израиль	2022/2023	Продолжается	Израиль принимает предварительный законопроект о расследовании незаконного использования программ, осуществляющих слежку полицией, хотя, как сообщает Middle East Monitor, ему нужно выдержать еще три голосования, чтобы официально стать законом. В конце 2023 года правительство Израиля опубликовало законопроект, который внесет поправки в закон 2022 года об агентстве внутренней безопасности Израиля и предлагает предоставить Шин Бет полномочия «проводить тайные обыски на компьютерах и мобильных телефонах с использованием инструментов наблюдения, таких как Pegasus, а также полный доступ к базам данных».
Испания	2022	Продолжается	В мае 2022 года Гонсало Бойе, юрист, представляющий многих каталонских лидеров, включая Карлеса Пучдемона, и сам ставший жертвой серии атак ПО Pegasus, подал иск в Мадриде против NSO, Q Cyber Technologies, дочерней компании в Люксембурге, OSY и старших должностных лиц этих предприятий.
Испания	2022	Продолжается	В апреле 2022 года, организации Mnium Cultural и the CUP, обратились с иском в суд Барселоны с просьбой расследовать нарушение их прав, конкретно назвав NSO Group и несколько дополнительных государственных учреждений Испании, включая Гражданскую гвардию и Национальную полицию. В июне 2022 года Роберто Вальверде, государственный прокурор Барселоны, специализирующийся на преступлениях, связанных с IT, постановил, что расследование деятельности NSO Group в Испании не может быть расследовано, но разрешил продолжить расследовать другие претензии CUP.
Испания	2022	Закрыто	Премьер-министр Испании Педро Санчес и министр обороны Маргарита Роблес сообщили, что их телефоны были заражены ПО Pegasus. По сообщениям из средств массовой информации Испанское правительство, подало жалобу в Национальный суд для дальнейшего расследования в мае 2022 года и пообещало реформировать испанские законы. В июне 2022 года Высший суд Испании вызвал генерального директора NSO Group для дачи показаний в качестве

			свидетеля по этому делу. В июле 2023 года расследование было отложено, а судебные власти сослались на «полное отсутствие сотрудничества» с Израилем
Испания	2022	Продолжается	Каталонские жертвы ПО Pegasus от NSO Group подали жалобы против NSO Group в Испании. В июле 2022 года испанский судья санкционировал расследование в отношении NSO Group.
Испания	2022	Продолжается	Министр по делам президента, парламентских отношений и демократической памяти Испании Феликс Боланос заявил, что правительство проведет «внутреннее расследование» в рамках Национального разведывательного центра по поводу использования ПО Pegasus в Испании. Это сопровождалось объявлением о том, что уполномоченный по правам человека Испании также начнет «независимое» расследование.
Франция	2022	Продолжается	Во Франции Международной федерацией прав человека (FIDH), Лигой прав человека (LDH) и франко-палестинским правозащитником Салахом Хаммури была подана жалоба против NSO Group.
Межамериканская комиссия по правам человека (IACHR)	2022	Продолжается	16 марта 2022 года Межамериканская комиссия по правам человека (IACHR) провела слушания по поводу незаконной слежки за журналистами и гражданским обществом в Сальвадоре.
Европейский союз	2022	Закрыто	Европейский парламент учредил комитет по расследованию «использования ПО Pegasus и аналогичных разведывательных программ для наблюдения». В июне 2023 года Европейский парламент вынес ряд рекомендаций Совету и Комиссии после расследования предполагаемых нарушений и ненадлежащего управления при применении законодательства Союза в отношении использования Pegasus и эквивалентных программ для наблюдения.
Венгрия	2022	Закрыто	Будапештская региональная следственная прокуратура начала расследование по факту использования ПО Pegasus «по подозрению в преступлении, заключающемся в несанкционированном сборе секретной информации». Венгерское национальное управление по защите данных и свободе информации также провело расследование использования ПО Pegasus в Венгрии, но не обнаружило никаких нарушений. Аргументация органа в значительной степени является

			секретной информацией и не была рассмотрена общественностью. В июне 2022 года Венгерская прокуратура прекратила расследование, сославшись на «отсутствие несанкционированного и секретного сбора информации или скрытного использования устройств».
Венгрия	2022	Продолжается	В январе 2022 года Венгерский союз гражданских свобод (HCLU) объявил, что подаст судебный иск от имени шести клиентов: журналистов Бригитты Чикаш, Давида Дерчени, Даниэля Немета и Саболча Паньи, бельгийско-канадского аспиранта и активиста Адриана Бодуэна, и шестого человека, пожелавшего сохранить анонимность. HCLU также объявил о планах представлять 36 клиентов в Европейском суде по правам человека. ЕСПЧ зарегистрировал жалобы в феврале 2023 года.
Европейская комиссия	2022	Закрыто	Венгерский союз гражданских свобод (HCLU) подал жалобу в Европейскую комиссию от имени Адриана Бодуэна, бельгийско-канадского активиста, ставшего объектом слежки во время учебы в Венгрии. В ответном письме от 17 августа 2022 года на имя его адвоката Комиссия заявила, что не компетентна вмешиваться, и отклонила дело Бодуэна.
Израиль	2022	Продолжается	После судебных процессов в Венгрии (см. выше) адвокат Эйтай Мак заявил, что он подаст иск в Израиле к генеральному прокурору страны как против NSO Group, так и против Министерства обороны Израиля. В 2023 году расследование, проведенное израильским прокурорским омбудсменом, судьей Менахемом Финкельштейном, определило, что генеральный прокурор Израиля задержал рассмотрение жалоб трех граждан Венгрии на группу NSO. Судья Финкельштейн поручил прокуратуре штата приложить усилия для завершения рассмотрения дела как можно скорее.
Польша	2024	Продолжается	В феврале 2024 года премьер-министр Польши объявил, что у него есть документация, подтверждающая, что государственные власти использовали Pegasus. Премьер-министр сказал, что попросил министра юстиции и генерального прокурора предоставить Дуде документы, которые «на 100% подтверждают покупку и использование Pegasus законным и незаконным образом». Парламент учредил специальную комиссию для расследования того, кто и против кого использовал Pegasus в годы правления предыдущего правительства.

Польша, Венгрия	2023	Закрыто	В мае 2023 года расследование Европейского парламента сообщило, что оно выявило «злоупотребления и программами в нескольких государствах-членах ЕС», включая «системные проблемы» в Польше и Венгрии.
Польша	2022	Продолжается	Комитет Сената Польши расследует использование ПО Pegasus в Польше против критиков правительства. В сентябре 2023 года комиссия Сената опубликовала отчет, в котором было установлено, что использование ПО против деятелей оппозиции сделало выборы 2019 года нечестными. Комиссия объявила, что проинформирует прокуроров о ряде предполагаемых преступлений, совершенных властями в связи с использованием ПО Pegasus.
Польша	2021	–	Прокурор Эва Вжосек, которая стала мишенью ПО Pegasus, подала уведомление в польский суд о предполагаемой кибератаке на ее мобильный телефон. В сентябре 2022 года суд обязал прокуратуру провести расследование слежки с помощью Pegasus.
Азербайджан	2021	Продолжается	По данным Azerbaijan Internet Watch, после разоблачений проекта Pegasus в Азербайджане был подан ряд жалоб и судебных исков в связи со слежкой Pegasus. В октябре 2023 года Media Defense подала четыре иска в Европейский суд по правам человека относительно использования ПО Pegasus правительством Азербайджана.
США	2021	Продолжается	В ноябре 2021 года Apple подала иск против NSO Group в федеральный суд США. Apple добивается постоянного судебного запрета NSO Group использовать программное обеспечение, сервисы или устройства Apple. Компания утверждает, что эксплойт, первоначально идентифицированный Citizen Lab (FORCEDENTRY), использовался для установки ПО Pegasus на устройства некоторых пользователей Apple. 24 января 2024 года федеральный суд отклонил просьбу NSO Group отклонить иск. NSO утверждала, что дело должно вестись в Израиле. Окружной судья Северной Калифорнии выразил мнение, что ресурсы затраченные на ведение судебного процесса в Калифорнии, не сопоставимы с ресурсами затраченными для Apple, если бы дело рассматривалось в Израиле.

Франция	2021	Продолжается	В июле 2021 года Центр по правам человека стран Персидского залива подал жалобу во Франции против NSO Group, утверждая, что компания «несет ответственность за вред, причиненный правозащитникам в регионе Ближнего Востока и Северной Африки (MENA) и за его пределами».
Индия	2021	Закрыто	В 2021 году в Верховный суд Индии был подан ряд петиций в связи с предполагаемым использованием ПО Pegasus индийскими властями против граждан Индии. В октябре 2021 года Суд издал приказ о назначении экспертно-технического комитета. Комитету, помимо прочих полномочий, было поручено провести расследование и определить, использовался ли Pegasus на телефонах или устройствах граждан Индии. В августе 2022 года Верховный суд сообщил, что комитет технических экспертов не смог обнаружить ПО Pegasus в 29 мобильных телефонах заявителей, но обнаружил иное вредоносное ПО в пяти из них.
Великобритания	2021	Продолжается	В августе 2021 года Bindmans LLP объявила, что ей «было поручено продолжить расследование претензий, которые потенциально могут быть поданы рядом лиц в связи с предполагаемым неправомерным использованием вредоносного ПО Pegasus от NSO Group иностранными правительствами». В группу заявителей входят активисты-правозащитники, ученые и лидеры организаций гражданского общества. 19 апреля 2022 года Bindmans LLP объявила, что три истца в феврале 2022 года направили потенциальным ответчикам письма с предварительными исками.
Франция	2021	Продолжается	Прокуратура Парижа начала расследование в отношении Pegasus 20 июля 2021 года после получения жалоб от Mediapart и двух ее репортеров на то, что за ними наблюдали из Марокко с помощью ПО Pegasus. Вскоре после этого еще 17 журналистов подали жалобы в прокуратуру Парижа. По данным организации «Репортеры без границ» (RSF), эти журналисты «знают или имеют серьезные основания опасаться», что правительства наблюдали за ними, используя ПО Pegasus от NSO Group в связи с их репортажной работой. RSF передала свое дело четырем специальным докладчикам ООН.

США	2020	Закрыто	Гада Уэисс, журналистка телеканала «Аль-Джазира», подала юридическую жалобу в федеральный суд США против ряда ответчиков, включая наследных принцев Саудовской Аравии и Объединенных Арабских Эмиратов, а также «Dark Matter», эмиратской компании по кибербезопасности. Она утверждает, что они организовали незаконную операцию по взлому и утечке данных против нее. В жалобе описывается «подозрительный процесс», который связан с ПО Pegasus от NSO Group. В марте 2022 года окружной суд Южного округа Флориды США отклонил дело. В апреле 2022 года Гада Уэисс подала апелляцию в Одиннадцатый окружной суд США. В ноябре 2022 года Уэисс добровольно отозвала свою апелляцию.
Испания	2020	Временно приостановлено	В 2020 году суд Барселоны начал расследование того, что в 2020 году ПО Pegasus было использовано против Роджера Торрента и Эрнеста Марагалла. В мае 2022 года судья Хосе Антонио Крус де Пабло временно приостановил расследование из-за отсутствия прогресса в получении информации о судебном поручении от израильских властей.
США	2019	Продолжается	29 октября 2019 года WhatsApp и Facebook подали жалобу на NSO Group / Q Cyber Technologies в Северном округе Калифорнии. Истцы утверждают, что в период с апреля 2019 года по май 2019 года ответчики использовали серверы WhatsApp, расположенные в США и других странах, для рассылки вредоносного ПО примерно на 1400 мобильных телефонов и устройств. Истцы требуют судебного запрета и возмещения ущерба в соответствии с Законом о компьютерном мошенничестве и злоупотреблениях и Калифорнийским законом о всеобъемлющем доступе к данным и мошенничестве (раздел 502 Уголовного кодекса), а также за нарушение контракта и незаконное проникновение в собственность движимого имущества. В апреле 2021 года Апелляционный суд девятого округа США отклонил требование NSO о защите в соответствии с законами о суверенном иммунитете и разрешил рассмотрение иска. В апреле 2022 года NSO Group подала апелляцию в Верховный суд США. В июне 2022 года Верховный суд попросил Министерство юстиции представить свое мнение о том, обладает ли NSO Group суверенным иммунитетом. 9 января 2023 года

			Верховный суд США отклонил ходатайство NSO Group.
Великобритания	2019	Закрыто	Ганем Альмасарир подал в Соединенном Королевстве, гражданский иск против Королевства Саудовской Аравии (KSA) о неправомерном использовании в отношении частной информации, преследовании и незаконном проникновении в товары. Ганем Альмасарир - известный саудовский диссидент, который живет в Соединенном Королевстве с 2003 года. Он считает, что правительство Саудовской Аравии использовало ПО Pegasus, приобретенное у NSO Group, и что они заразили им его мобильные телефоны, чтобы изменять, извлекать и записывать всю информацию, хранящуюся на этих устройствах и передаваемую через них. Он также считает, что ПО позволило KSA получить доступ к микрофону и камере телефона, чтобы видеть и слышать, что он делает. Иск был подан 4 ноября 2019 года. В январе 2020 года Верховный суд Великобритании заявил, что дело может быть продолжено. В августе 2022 года Верховный суд Великобритании отклонил попытку Саудовской Аравии использовать положения об иммунитете государства для блокирования иска в связи с обвинениями в использовании ПО Pegasus и разрешил продолжить рассмотрение дела. KSA подало заявление об обжаловании решения Верховного суда и постановления о расходах. В мае 2023 года Апелляционный суд удовлетворил апелляцию на решение суда, но отказался изменять порядок возмещения расходов. После невыполнения саудовским режимом постановлений суда Апелляционный суд обязал KSA произвести выплату в размере 210 000 фунтов стерлингов или отклонить его апелляцию без дальнейшего распоряжения. KSA не заплатила, и впоследствии, 27 ноября 2023 года, апелляция KSA на решение 2022 года была отклонена. В декабре 2023 года KSA отстранило свою команду юристов от представления интересов в этом разбирательстве.

Израиль	2019	Закрыто	14 мая 2019 года израильские заявители подали апелляцию на решение Министерства обороны Израиля не отзывать экспортную лицензию NSO Group в связи с нападением на сотрудника Amnesty International. Amnesty International поддержала петицию и представила письменные показания под присягой. В июле 2020 года суд Тель-Авива отклонил эту попытку заставить Министерство обороны Израиля отклонить лицензию NSO Group.
Израиль	2018	Продолжается	Омар Абдулазиз подал иск в Израиле против NSO Group. Согласно информации, полученной из СМИ, в иске утверждается, что NSO Group помогла королевскому суду Саудовской Аравии завладеть его смартфоном и наблюдать за его перепиской с убитым Джамалем Хашогги. NSO Group опубликовала заявление о том, что ее продукты были «лицензированы исключительно для предоставления правительствам и правоохранительным органам возможности законно бороться с терроризмом и преступностью», и что контракты на использование разведывательных программ группы NSO «предоставляются только после полной проверки и лицензирования правительством Израиля». Компания также добавила, что не приемлет «неправильного использования» своих продуктов и что, если есть «подозрение на неправильное использование», компания расследует это и предпринимает соответствующие действия, включая приостановление или расторжение контракта. Иск был подан Алаа Махаджной, израильским юристом, в сотрудничестве с Мазеном Масри, преподавателем Лондонского городского университета. Адвокаты заявили в судебных документах, что намерены доказать, что разоблачение сотрудничества между Абдулазизом и Хашогги «в значительной степени способствовало принятию решения об убийстве мистера Хашогги». В июне 2020 года израильский судья отклонил ходатайство NSO Group об отклонении дела и их призыв провести судебное разбирательство в тайне и обязал NSO Group оплатить судебные издержки Абдулазиза. Группа NSO заявила, что подаст апелляцию.

Израиль и Кипр	2018	Продолжается	Мексиканские журналисты и активисты гражданского общества подали иск против NSO Group в Израиле (гражданин Катара также подал иск против NSO Group на Кипре). Согласно информации, полученной из СМИ, эти судебные иски включают документы и электронные письма, которые прямо оспаривают неоднократные утверждения компании о том, что она не несет ответственности за какую-либо незаконную слежку, проводимую правительствами, которые покупают ее разведывательные программы. Эти судебные иски также были поданы Алаа Махаджной и Мазеном Масри.
Израиль	2018	Продолжается	В июле 2018 года Министерство юстиции Израиля заявило, что бывшему сотруднику NSO Group предъявлены обвинения в краже интеллектуальной собственности и попытке продать их за 50 миллионов долларов через Даркнет и который может нанести ущерб государственной безопасности. Министерство юстиции заявило, что, согласно показаниям, собранным по делу, действия бывшего сотрудника «поставили под угрозу NSO Group и могли привести к его краху», и представляли угрозу государственной безопасности.
Мексика	2017	N/A	Федеральное расследование мексиканских властей по факту использования ПО Pegasus в Мексике было объявлено мексиканским правительством в 2017 году. Однако его усилия, похоже, зашли в тупик. Согласно информации, полученной из СМИ, известно, что власти США, к которым обратились мексиканские следователи, считают это фиктивным расследованием и отказались участвовать.

Конкуренты NSO GROUP на рынке

Весь мир увлеченно следит за тем, как публично хоронят NSO Group с печально известным разведывательным ПО Pegasus. Но скорее всего, дело вовсе не в борьбе за демократию. Права человека - товар на рынке разведывательных технологий, а Израиль вежливо попросили подвинуться.

Если применение Pegasus носило целевой характер и реализовывалось по линии спецслужб, то их американские коллеги **Anomaly Six** отслеживают до 3 миллиардов мобильных устройств по всему миру в моменте.

За несколько месяцев до начала спецоперации РФ на Украине компания объединилась с **Zignal Labs**, которые специализируются на наблюдении в соцсетях. Консолидированный ресурс позволил им одним щелчком отследить передвижения российских войск в ходе развертывания вдоль границы с Украиной. Выделить места обучения, дислокации, проживания военнослужащих, а также окружение, связи и маршруты передвижений. В ходе другого кейса аналогичным образом проводился контроль за атомной подводной лодкой КНР.

A6 продемонстрировали результаты мониторинга в районе расположения ЧВК «Вагнер» в РФ, на основе которого были выявлены командировки бойцов Ливию, Конго и другие точки. При этом **Zignal** давали и содержательную оценку активности пользователей в той или иной местности на основе публикаций в соцсетях, легко опровергая, к примеру, легенду об учениях.

A6 реализуют от 30 до 60 пингов местоположения на устройство в день, покрывая 230 миллионов устройств в день и добавляя в систему почти 2,5 триллиона локаций ежегодно. В отличие от конкурентов, собирающих местоположения через Bluetooth и Wi-Fi-соединения телефона, компания использует сеть GPS. Каждой локации соответствует пользовательский профиль из базы, включающей более чем 2 миллиардов записей личных данных, которыми пользователи делятся при регистрации в приложениях.

Интерфейс ПО визуализирует локаций пользователей в стиле Google Maps, осуществляя поиск как по заданному местоположению (району, городу или даже стране), так и в отношении конкретного абонента.

Виртуозы разведки также показали, насколько уязвимы их собственные спецслужбы. Отмониторив штаб-квартиру АНБ в Форт-Мид, штат Мэриленд, и штаб-квартиру ЦРУ в Лэнгли, штат Вирджиния, операторы **Anomaly Six** смогли срисовать 183 устройства, посетившие обе локации, а также раскрыть их перемещения за рубежом по линии разведки. По возвращении в США одного из объектов контроля проследили прямо до дома.

Anomaly Six поставила на поток сбор данных о местоположении пользователей мобильных приложений, запущенный конвейер позволил им отслеживать сотни миллионов людей по всему миру онлайн. Для этих целей используют SDK. В свою очередь, Zignal Labs, имея эксклюзивную технологию парсинга, взяли фактически под контроль публичные коммуникации в Twitter.

Заключение

Аналитический центр Observer Research Foundation (ORF), базирующийся в городе Дели, недавно выдвинул тезис о необходимости международного реагирования на действия так называемых «кибернаёмников». В числе примеров таких наёмников приводятся известная северокорейская группировка Lazarus и израильская компания NSO Group, занимающаяся продажей разведывательного ПО.

Автор отчёта - Фитри Бинтанг Тимур утверждает, что такие группировки следует рассматривать как наёмников в сфере кибербезопасности. Она ссылается на определение наёмников по Женевской конвенции как «субъектов, мотивированных финансовой или материальной выгодой, готовых воевать за страну заказчика». В современном мире это означает использование информационных технологий и сетей для проведения кибероперaций.

Как примеры таких действий, Тимур привела разработку и распространение вредоносного ПО группой Lazarus по заказу правительства Северной Кореи, а также продажу израильской компанией NSO Group своего разведывательного программного обеспечения Pegasus правительствам многих стран, несмотря на его нелегитимность и спорный статус.

Отчёт подчёркивает, что рынок кибернаёмников растёт, так как они позволяют государствам усиливать свои наступательные возможности, сохраняя при этом «правдоподобное отрицание вовлечённости за счёт неузнаваемости».

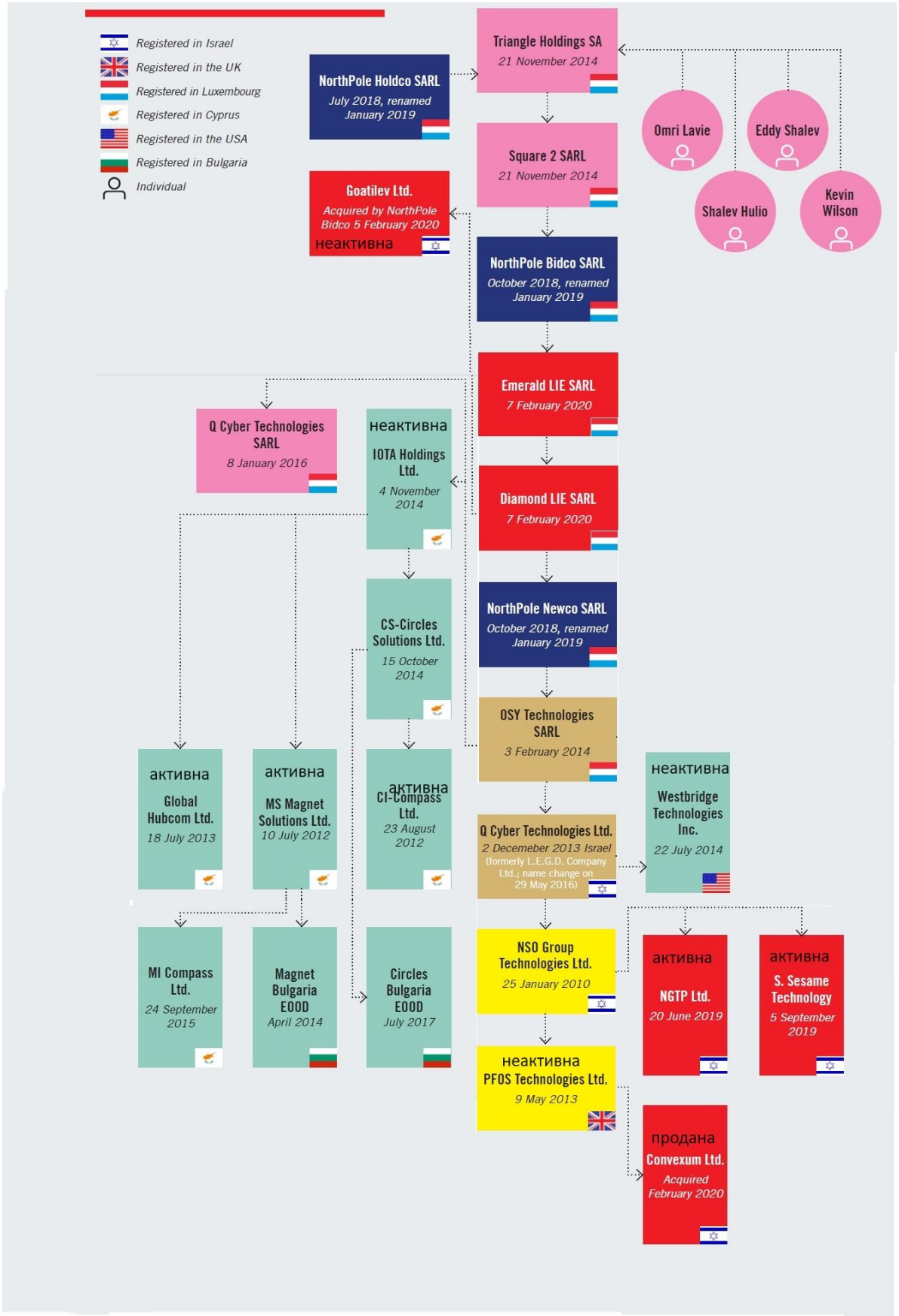
Также отмечается, что использование кибернаёмников экономически выгодно: они не требуют отдела кадров, обучения и других затрат на персонал. Страны, не имеющие возможности содержать собственные подразделения национальных хакеров, могут нанимать кибернаёмников для достижения своих целей.

Тимур призывает к разработке законодательства, которое бы сочетало использование разведывательных и цифровых средств с обязанностями по соблюдению прав человека. Она также подчёркивает необходимость установления стандартов, согласно которым действия кого бы то ни было в интересах чьей-либо национальной безопасности должны в обязательном порядке уважать эти права.

В качестве примера упоминается ситуация с NSO Group, когда Еврокомиссия решила не вмешиваться в использование государствами-членами ЕС их разведывательного ПО Pegasus, классифицированного как инструмент «национальной безопасности». Однако это ПО использовалось для слежки за политиками, журналистами, бизнесменами, активистами, учёными и другими лицами, представляющими малую угрозу безопасности, но с большой вероятностью создающими политикам лишние хлопоты.

Отчёт Тимур завершается призывом к гражданам требовать от правительств и бизнеса ответственности за привлечение кибернаёмников. Девушка также упомянула, что гражданские общественные группы уже давно предпринимают активные действия через судебные иски, требуя от любых похожего рода объединений большей прозрачности.

Приложение 1. Схема роста NSO Group



Приложение 2: Случаи использования Pegasus

Страна	Год использования	Марка ПО	Страна изготовитель
Азербайджан	2019-2021	NSO Group	Израиль
Бахрейн	2016-2018, 2020, 2021	NSO Group	Израиль
Бангладеш		NSO Group	Израиль
Бельгия		NSO Group	Израиль
Джибути		NSO Group	Израиль
Египет	2021	NSO Group	Израиль
Сальвадор	2020-2021	NSO Group	Израиль
Эстония	2018-2022	NSO Group	Израиль
Германия	2019-2021	NSO Group	Израиль
Гана		NSO Group	Израиль
Венгрия	2017-2022	NSO Group	Израиль
Индия	2017-2021	NSO Group	Израиль
Индонезия	2021	NSO Group	Израиль
Израиль		NSO Group	Израиль
Иордания	2019-2021	NSO Group	Израиль
Казахстан		NSO Group	Израиль
Кения	2015	NSO Group	Израиль
Мексика	2016-2018, 2021	NSO Group	Израиль
Марокко	2017-2021	NSO Group	Израиль
Нидерланды	2019	NSO Group	Израиль
Панама	2012-2014	NSO Group	Израиль
Польша	2017-2019	NSO Group	Израиль
Руанда	2016-2020	NSO Group	Израиль
Саудовская Аравия	2017-2018	NSO Group	Израиль
Испания	2015, 2017-2020	NSO Group	Израиль
Таиланд	2020-2021	NSO Group	Израиль
Того	2019	NSO Group	Израиль
Уганда	2019-2021	NSO Group	Израиль
ОАЭ	2016	NSO Group	Израиль
Узбекистан	2018	NSO Group	Израиль

По некоторым данным 2018 года, было выявлено 45 стран с подозрением на заражение разведывательным программным обеспечением Pegasus и как минимум 33 клиента NSO.

Operator name	Dates operator was active	Suspected country focus	Political themes?	Suspected infections
RECKLESS-1	Sep 2016 – Jun 2017	Mexico	Yes	–
RECKLESS-2	Oct 2016 – Jun 2017	Mexico	Yes	–
MAYBERECKLESS	Sep 2017 – present	–	–	Mexico
PRICKLYPEAR	Oct 2016 – present	Mexico	–	Mexico, USA (Arizona)
AGUILAREAL	Sep 2016 – present	Mexico	–	Mexico
MACAW	Nov 2017 – present	Honduras	Yes	–

Operator name	Dates operator was active	Suspected country focus	Political themes?	Suspected infections
REDLIONS	Mar 2017 – present	–	Yes	Togo
ATLAS	Aug 2017 – present	Morocco	Yes	Algeria, Cote d'Ivoire, France, Morocco, Tunisia, UAE
GRANDLACS	Jun 2017 – present	Great Lakes region of Africa	Yes	Kenya, Rwanda, South Africa, Uganda
MULUNGUSHI	Feb 2018 – present	Zambia	–	South Africa, Zambia
AK47	Dec 2016 – Jul 2017	Mozambique	–	–
MACAW	Nov 2017 – present	Honduras	Yes	–

Operator name	Dates operator was active	Suspected country focus	Political themes?	Suspected infections
ORZELBIALY	Nov 2017 – present	Poland	–	Poland
EDELWEISS	Jul 2017 – present	Switzerland	–	Switzerland
5LATS	Mar 2018 – present	Latvia	–	Latvia
TURUL	Feb 2018 – present	Hungary	–	–
CHEQUY	Nov 2016 – present	Croatia	–	–
MACAW	Nov 2017 – present	Honduras	Yes	–

Operator name	Dates operator was active	Suspected country focus	Political themes?	Suspected infections
PEARL	Jul 2017 – present	Bahrain	Yes	Bahrain, Qatar
FALCON	Oct 2016 – present	UAE	Yes	UAE
BABYFALCON	May 2018 – present	GCC Region	–	UAE
MAYBEFALCON	Sep 2016 – present	–	–	UAE
BLACKBIRD	Sep 2016 – present	–	–	Greece, Jordan, Kuwait, Libya, Qatar, UAE, UK, USA, Yemen
KINGDOM	Oct 2017 – present	Saudi Arabia	–	Bahrain, Canada, Egypt, France, Iraq, Jordan, Lebanon, Morocco, Qatar, Saudi Arabia, Turkey, UK
MIDDLE	Sep 2016 – present	–	–	France, Jordan, Lebanon, Oman, Qatar, Tunisia, Turkey, UAE
OLIVE-1	Jun 2017 – present	–	–	Israel
OLIVE-2	Aug 2017 – present	–	–	Israel
OLIVE-3	Dec 2016 – present	–	–	Israel
OLIVE-4	Oct 2016 – present	–	–	Israel
DOME	Mar 2018 – present	–	–	Israel, Netherlands, Palestine, Qatar, Turkey, USA

Operator name	Dates operator was active	Suspected country focus	Political themes?	Suspected infections
CHANG	Jan 2018 – present	Asia	–	Thailand
GANGES	Jun 2017 – present	–	Yes	Bangladesh, Brazil, Hong Kong, India, Pakistan
MERLION	Dec 2016 – present	–	–	Singapore
TULPAR	Feb 2017 – present	Kazakhstan	–	Kazakhstan
SYRDARYA	Sep 2016 – present	Uzbekistan	–	Kazakhstan, Kyrgyzstan, Tajikistan, Turkey,
Uzbekistan	Nov 2017 – present	Honduras	Yes	–

Приложение 3: Конкурирующие продукты слежки

Продукт	Страна производитель
Magnet Forensics	Канада
OpenText	Канада
EaseUS	Китай
Fiberhome	Китай
Meiya Pico	Китай
Resonant	Китай
SalvationData	Китай
Zhongke Ronghui Security Technology	Китай
DigiTask	Германия
FinFisher	Германия
iMyFone	Гонконг
Black Cube	Израиль
Candiru	Израиль
Cellebrite	Израиль
Cyberbit	Израиль
Hacking Team	Израиль
Paragon	Израиль
Quadream	Израиль
Toka	Израиль
Cytrox	Израиль, Венгрия
eSurv	Италия
Hacking Team	Италия
RCS Labs	Италия
SecurCube	Италия
Dark Caracal	Ливан

Elcomsoft	Россия
Oxygen Software	Россия
Mollitiam	Испания
MSAB	Швеция
AccessData	США
Grayshift	США
Paraben	США
Passware	США
Sillicon Forensics	США
Sirchie	США
Susteen	США
SysTools	США
BlackBag	США, Израиль

В случае возникновения вопросов относительно предоставленного отчета просим обращаться дополнительно.