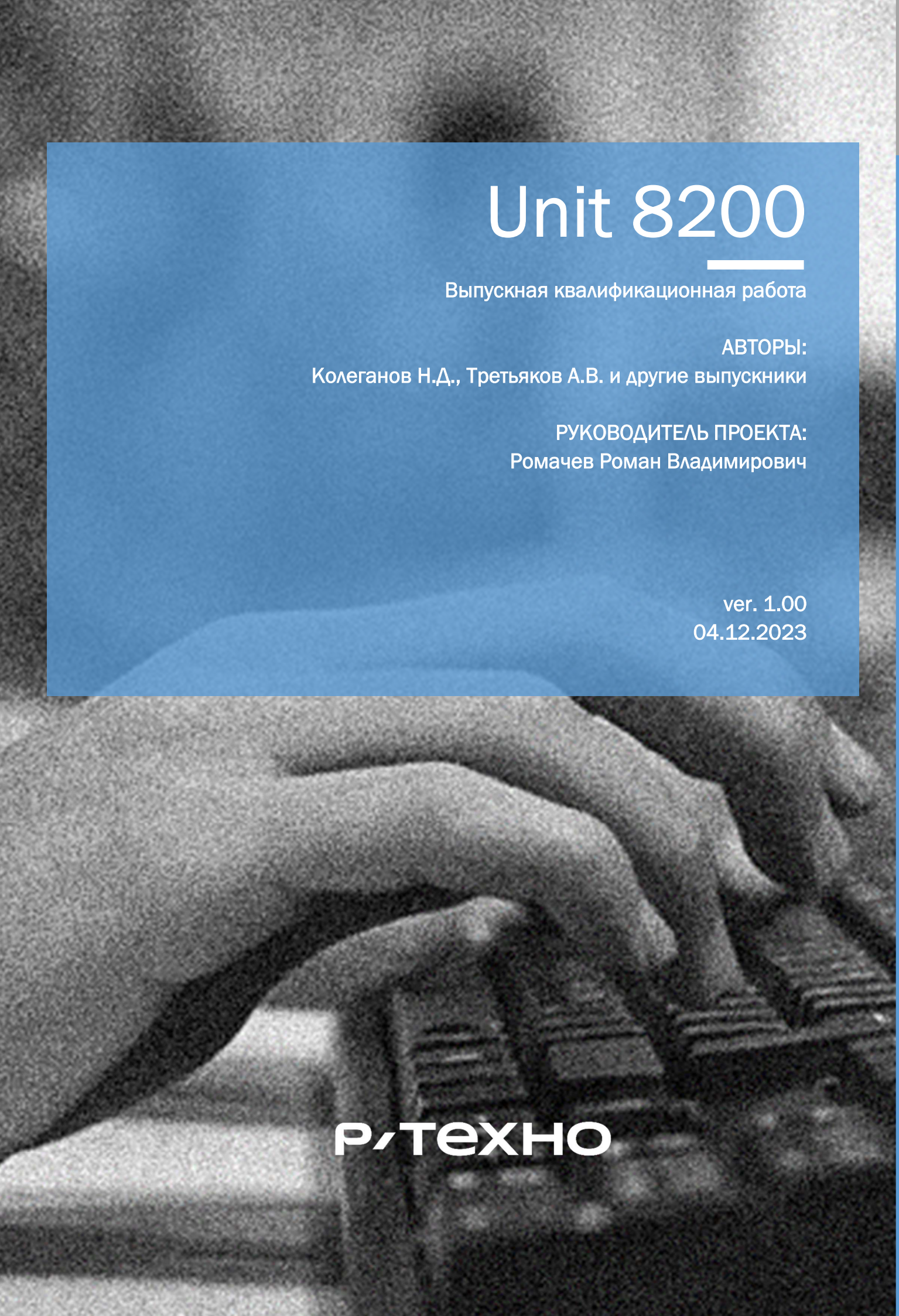
Unit 8200

Выпускная квалификационная работа

АВТОРЫ:
Колеганов Н.Д., Третьяков А.В. и другие выпускники

РУКОВОДИТЕЛЬ ПРОЕКТА:
Ромачев Роман Владимирович

ver. 1.00
04.12.2023



РТЕХНО

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

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

СОДЕРЖАНИЕ

Выводы

Подразделение 8200 – израильское подразделение радиоэлектронной разведки Управления военной разведки Армии обороны Израиля (АМАН). Помимо собственно РЭР, также участвует в контрразведывательных операциях, кибероперациях, осуществляет оценку разведывательных данных. Согласно ряду источников, является **одним из крупнейших подразделений РЭР в мире.** Имеет тесные связи с крупными компаниями в сфере ИТ и финтеха.

Считается **одной из лучших разведывательных служб в мире**, а также одним из лидеров среди мировых спецслужб по **уровню технического оснащения**. Подразделение осуществило **ряд успешных операций на территории Палестины, Ирана, Северной Африки, Европы** и других регионов.

Одним из ключевых направлений деятельности подразделения является кибеpразведка, включая проведение кибероперaций с **созданием и распространением вредоносного ПО**. При этом не все кибератаки, приписываемые подразделению, удалось достоверно с ним связать.

Тесно сотрудничает со спецслужбами других стран, в первую очередь США, Великобритании и Канады. Одним из ведущих партнеров подразделения является **Агентство национальной безопасности США.**

Ветераны подразделения сохраняют с ним тесную связь, а также активно создают технологические компании и (или) строят карьеру в крупных корпорациях. Таким образом подразделение имеет связи практически со всеми крупными организациями в сфере ИТ и ИБ, а также **имеет возможность оказывать влияние через создаваемые и распространяемые этими организациями технологии и решения**.

Подразделение 8200 **активно работает с молодежью**, оказывает помощь и поддержку в обучении школьников и студентов, уделяя особое внимание высоким технологиям, программированию и иностранным языкам (преимущественно арабскому).

Сильные стороны Подразделения 8200:

- Значительные человеческие и финансовые ресурсы;
- Культура гибкого мышления, находчивости, принятия риска, быстрой адаптации, командной работы и плоской иерархии;
- Связи с политическими институтами и общественными организациями;

- Инновационные разработки и ноу-хау, тесное сотрудничество с научными организациями;
- Партнерство с частными компаниями и корпорациями;
- Нетворкинг: наличие сети из бывших сотрудников во всех значимых технологических компаниях мира;
- Сильный образ подразделения, выстроенная внутренняя и идеологическая культура.

Слабые стороны Подразделения 8200:

- Внутренние противоречия, отсутствие единства как минимум среди бывших сотрудников Подразделения по ряду вопросов, связанных с этикой. В 2014 году 43 резервиста осудили в открытом письме слежку за палестинцами, не причастными к военным действиям и терроризму.
- Чрезмерная бюрократизация, которая может негативно отразиться на эффективности процессов и инновационном развитии;
- Набор новобранцев из строго ограниченного круга (элитные учебные заведения, преимущественно в Тель-Авиве). Вследствие этого Подразделение упускает талантливые кадры, не входящие в «избранный круг»;
- Сложная адаптация бывших сотрудников к гражданской жизни и работе после нескольких лет службы в Подразделении;
- Репутационные риски и скандалы, в центре которых время от времени оказывается Подразделение, несмотря на сильный бренд в целом;
- Рост стоимости технологий и оборудования, необходимых для работы Подразделения, приводит к увеличению издержек.

Методы работы Подразделения 8200 и его связи с бизнесом и научными организациями имеют и более глобальные последствия как для Израиля, так и для всего мира. Подразделение 8200 считается инкубатором для будущих очень успешных стартапов в области кибербезопасности, технологических венчурных капиталистов и экспертов по кибербезопасности. **Эта репутация, наряду с патриотизмом, является основной мотивацией присоединиться к Подразделению 8200**. По сравнению с традиционными гражданскими и частными инкубаторами, военная культура, миссии и сеть Подразделения 8200 **позволяют развивать конкретные лидерские, технические и предпринимательские навыки и способствуют высокому уровню доверия между выпускниками.**

Идентификационные данные

Unit 8200 (Подразделение 8200) – израильское подразделение радиоэлектронной разведки (РЭР). Помимо собственно РЭР, также участвует в контрразведывательных операциях, кибероперациях, осуществляет оценку разведывательных данных.

Иврит: יחידה 8200 (Yehida shmone matayim).
Английский язык: Unit 8200.

Из публикаций открытых источников на военную тематику (в большинстве своем англоязычных), Подразделение 8200 иногда называют Центральным подразделением разведывательного корпуса по сбору информации (Central Collection Unit of the Intelligence Corps), а также Израильским национальным подразделением SIGINT (Israeli SIGINT National Unit, ISNU).

Изначально называлось Разведывательным подразделением №2, затем – №515 и №848. Нынешнее название получило в ходе или сразу после арабо-израильской войны 1973 г. (т.н. войны Судного дня).

Штаб-квартира

С 1954 г. штаб-квартира Подразделения расположена недалеко от развязки Глилот между Тель-Авивом, Герцлией и Рамат-ха-Шароном, возможно, непосредственно на военной базе Глилот. Ранее располагалась в городе Яффа и недолгое время – в Тель-Авиве.

Крупнейшая база подразделения расположена в пустыне Негев недалеко от кибуца Урим в городе Беер-Шева.

Численность

Точная численность засекречена. По некоторым данным в настоящий момент количество офицеров и военнослужащих, проходящих срочную службу, составляет более 500 человек на постоянной основе. Кроме того, ветераны подразделения 8200, как и все другие ветераны ЦАХАЛ обязаны служить в резерве до трех недель каждый год, пока им не исполнится 40 лет. Таким образом, за счет резервистов

общая численность подразделения 8200 достигает нескольких тысяч человек (по версии ряда источников – около 5000).

Основные виды деятельности

Основным видом деятельности Подразделения 8200 является радиоэлектронная разведка, включающая в себя сбор и перехват радиосигналов, декодирование зашифрованной информации, прослушивание телефонных разговоров, в том числе первых лиц других государств, выведение из строя инфраструктуры противника, в том числе средств наведения, навигации, ПВО и т.д. Особое внимание уделяется наблюдению за палестинскими территориями.

По некоторым данным, подразделение активно участвует в кибероперациях, в том числе создает и распространяет вредоносное программное обеспечение.
Помимо разведывательной деятельности, также участвует в контрразведывательных операциях. Одним из основных видов деятельности является разведка по открытым источникам (OSINT).

Руководство и структура

Действующий командир подразделения имеет звание бригадного генерала, его личность засекречена.

Подразделение 8200 входит в Управление военной разведки (АМАН) Армии обороны Израиля (ЦАХАЛ).

В состав подразделения входят следующие структурные единицы.

- **Подразделение 81**. Одно из наиболее засекреченных в составе Подразделения 8200. Специализируется на исследованиях и поставках самых современных технологий (как правило, интегрированных программно-аппаратных комплексов) израильским военнослужащим. По некоторым оценкам, в состав подразделения входит около 1000 солдат, или примерно пятая часть военнослужащих Подразделения 8200.

  Подразделение не полагается на внешние разработки и технологии. Все технологические системы Подразделения, от аналитических систем до разработок на основе искусственного интеллекта, а также решений для перехвата информации, разрабатываются и встраиваются собственными силами.

- **Гедасим (Gedasim), или операционный блок 8200 (מבצעית יחידה 8200).** Подразделение выполняет функцию сбора разведданных на местах в режиме реального времени и передачи их, опять же в режиме реального времени, частям

действующей армии. В его задачу входит подготовка подразделений радиоэлектронной разведки, которые при необходимости будут придаваться частям действующей армии в ходе военных действий и (или) специальных операций.

- **Подразделение воздушной разведки (Mauf Rahav, יחידת מעוף רחב)**. Осуществляет сбор и обработку информации в целях защиты воздушного и морского пространства страны, действует совместно с подразделениями ВВС и ВМФ.

Ранее в состав Подразделения также входило **Подразделение Хацав (англ. Unit Hatzav, ивр. יחידת חצב)**, специализировавшееся на разведке по открытым источникам. Расформировано в декабре 2021 года, его военнослужащие распределены по другим единицам Подразделения 8200.

Согласно ряду источников, в Подразделение также входит киберцентр, выполняющий исследования в сфере кибербезопасности и искусственного интеллекта, аналитический центр, радиоэлектронный центр, технологический центр и школа подготовки персонала.

Инфраструктура

Будучи нацеленным на радиоэлектронную разведку, Подразделение 8200 располагает большим количеством баз, подавляющее большинство которых остается засекреченным.

Помимо крупнейшей базы Урим, на территории которой находятся как минимум 30 радиолокационных антенн, у Подразделения также есть базы в Оре, Тель-Авиве (Голанские высоты), на горе Хермон и в Ум-Хашибе. Подразделение также управляет совместной базой с АНБ в Офрите (Восточный Иерусалим).

Кроме того, в г. Беер-Шева расположен крупный технопарк Advanced Technologies Park (ATP), официально позиционируемый правительством Израиля как будущий «киберцентр Западного полушария». Помимо научных центров, государственных организаций и частных компаний из Израиля и других стран, в парке представлены также военные структуры. В 2020 году парк стал новой штаб-квартирой Разведывательного управления и отдела связи Армии обороны Израиля.

История создания

Время и цели создания

Начало прослушивания телефонных разговоров относится еще к периоду британского мандатного управления в Палестине (1920-1948 гг.), а первое известное подразделение, занимавшееся радиоперехватом, было создано в 1929 г. и называлось Шин Мем 2 (Shin Mem 2). В это время перехват и прослушивание разговоров носило характер скорее не систематической деятельности, а единичных операций. Деятельность прослушивающих подразделений поддерживалась и курировалась Хаганой – подпольной военной организацией, которая провозглашала своей целью защиту еврейского населения в Палестине и создание независимого государства Израиль.

В 1939 г. британское правительство приняло документ, известный как «Белая книга 1939 года», существенно ограничивавший евреям возможность иммиграции на территорию Палестины и приобретение там земли. Важной частью сопротивления со стороны еврейского населения Палестины стало создание подпольных военизированных организаций, в том числе нацеленных на перехват информации из британских военных и полицейских подразделений. Один из таких отрядов, впоследствии ставший основой Подразделения 8200, действовал в Тель-Авиве.

Во время арабо-израильской войны 1947-1947 гг., также известной как Война за независимость Израиля, еврейская сторона активно использовала методы РЭР для перехвата информации, передаваемой по системам связи для координирования арабских войск. В осажденном Иерусалиме в этот период действовала т.н. «Тайная служба расшифровки». В 1948 г. ее объединили с отрядом, действовавшим в Тель-Авиве, что фактически положило начало существованию подразделения, сегодня известного как Подразделение 8200. К тому моменту подразделение насчитывало около 250 человек.

В 50-60-е гг. XX века подразделение активно осваивало компьютерные технологии и совершенствовало методы РЭР.

Подразделение участвовало во всех значимых военных конфликтах Израиля, в том числе в Шестидневной войне 1967 г., Израильско-египетской войне 1967-1970 гг., а также Войне Судного дня 1973 г., после окончания которой и получило свое нынешнее название.

К периоду Войны Судного дня относится один из наиболее известных провалов подразделения. Информация о том, что коалиция арабских государств готовит

нападение, была передана военным слишком поздно (за несколько часов до начала атаки), что не позволило должным образом к нему подготовиться. Кроме того, объект подразделения на заставе Хермон был захвачен сирийскими отрядами, в результате чего 13 солдат были взяты в плен. Среди них был и офицер разведки Амос Левинберг, который впоследствии раскрыл нападавшим секретную информацию, в том числе и о Подразделении 8200.

В XXI в. подразделение продолжает выполнять различные задачи в рамках палестино-израильского конфликта, борьбы с радикальными исламистскими организациями, а также сотрудничества со специальными службами других стран, в основном США и Великобритании. Подразделение также занимается разработкой цифровых технологий и продуктов как военного, так и двойного и гражданского назначения (например, систем дистанционного обучения для школьников и студентов во время пандемии коронавируса).

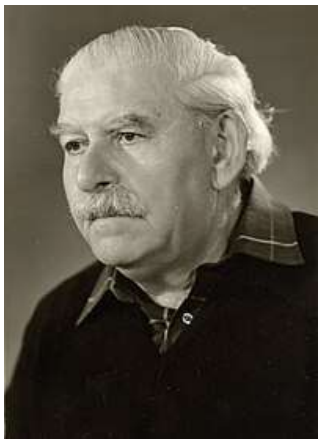
Ключевые лица на этапе создания

Мордехай Альмог (אלמוג מרדכי), 1917-2005 – основатель Подразделения 8200 и его первый командир. Родился в г. Проскурове Российской империи (ныне г. Хмельницкий на Украине), в 1919 г. вместе с семьей иммигрировал в Сербию, в 1933 г. – в Палестину, на земли современного Израиля, где присоединился к движению Хагана. От имени Еврейского агентства (Сохнут) был направлен на курсы связи в британской полиции, некоторое время занимал должность радиста в полиции Цфата. Уволился из британской полиции после обвинения в убийстве араба, хотя был оправдан. После отставки создал в Тель-Авиве подразделение прослушки и радиоперехвата. После ухода из подразделения в 1950-х гг. был назначен руководителем разведывательного подразделения АМАНа, затем перешел в Моссад. После ухода из Моссада он занялся туристическим бизнесом, поощрял развитие въездного туризма в Израиль и стал председателем Ассоциации турагентов Израиль. В 1999 г. Альмогу было присвоено звание бригадного генерала.

Жена – Хана Яновер. В браке родились 2 дочери.

Реувен Блюм (בלום ראובן), 1924-2015 – один из основателей будущего Подразделения 8200, в 1961-1966 – командир подразделения. Родился в Мюнхене (Германия), в юности иммигрировал в Израиль вместе с семьей. В 1940-1944 гг. служил в еврейско-иорданском корпусе, входящим в состав частей британской армии, действовавших на подмандатной территории. Во время военной службы освоил работу с радиосвязью и прошел обучение на техника-электронщика. В дальнейшем изучал физику и математику в Еврейском

университете в Иерусалиме. В 1948 г. вступил в «Тайные расшифровки», где отвечал за техническое обеспечение. С 1953 г. возглавил технический отдел подразделения, с 1959 г. стал исполняющим обязанности, а с 1961 г. – официальным командиром подразделения. Внес большой вклад в технологическое развитие подразделения. При Блюме были созданы и усовершенствованы базы в центре и на севере страны, открыты курсы довоенной подготовки в области беспроводных технологий, значительно выросли вычислительные мощности подразделения.

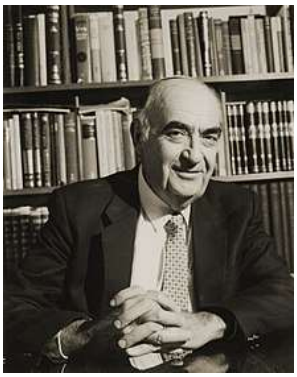


Яаков Хаим (Ганс) Полоцкий (פּוֹלוֹצקי (הַנס)חיים יעקב), 1905-1991 – лингвист, языковед, специалист по дешифрованию, стоявший у истоков будущего Подразделения 8200. Родился в Цюрихе (Швейцария), учился и вел научную деятельность в Берлине и Геттингене, специализировался на исследованиях и переводах древних текстов на греческом, коптском, сирийском и арабском языках. Переехал в Палестину после прихода к власти нацистов. В Еврейском университете основал факультет лингвистики, возглавил факультет гуманитарных наук, вернулся к изучению египетского языка, а также начал заниматься современными семитскими языками. Во время Войны за независимость вступил в «Тайную службу расшифровки», где специализировался на взломе шифров.

Полоцкий стал одним из крупнейших исследователей семитских языков в XX в. В 1959 г. был избран членом Израильской национальной Академии наук. Лауреат премии Ротшильда в области гуманитарных наук, премии Израиля в области гуманитарных наук, а также премии Харви.

Иегошуа Блау (בלאו יהושע), 1919-2020 – лингвист, профессор кафедры арабского языка и литературы Еврейского университета в Иерусалиме, Президент Академии иврита, один из величайших исследователей средневековых семитских языков. Стоял у истоков Подразделения 8200. Родился в Трансильвании, впоследствии вместе с семьей перебрался в Австрию, где изучал арабский язык. В 1938 г. эмигрировал на Землю обетованную где продолжил изучение арабского языка и иврита. Окончил Еврейский университет, работал школьным учителем. Во время Войны за независимость вступил в «Тайную службу расшифровки», где специализировался на взломе кодов. После войны занимался научными исследованиями, в т.ч. под руководством Яакова Полоцкого. В качестве приглашенного преподавателя вел занятия в Университете Беркли, Гарварде, Университете Нью-Йорка и т.д.

Давид Цви Беннет (בֶּנֶט (הֶרְטְוויג) צבי דוד), 1893-1973 – историк-религиовед, исследователь религиозной философии ислама и иудаизма. Стоял у истоков будущего Подразделения 8200, где занимался криптоаналитикой. Родился в Кротошине (Германская империя, в настоящее время – Польша). Один из основателей Еврейского университета, заложивший основы изучения еврейского арабского языка, учитель Иегошуа Блау.



Шломо Морг (מורג שלמה), 1926-1999 – языковед, один из ведущих специалистов в области иудаики. Стоял у истоков будущего Подразделения 8200, занимался криптоанализом. Ученик Яакова Полоцкого и Давида Цви Беннета.

Финансовая деятельность

Финансирование и его основные источники

Основное финансирование осуществляется за счет государственного бюджета. Общий военный бюджет Израиля – порядка 17 млрд долларов США (по состоянию на 2018 г.).

На начальном этапе существования финансирование организации было довольно скудным, и в своей работе подразделение использовало старое американское оборудование. Одним из достижений основателя подразделения Мордехая Альмога стало то, что он сумел убедить руководство выделить финансирование в размере 1500 фунтов стерлингов.

В 1950 году подразделению был выделен бюджет в размере 15 000 долларов США и дополнительно 110 000 долларов США на первоначальное электронное оборудование – в основном излишки американских запасов. В сегодняшней валюте это было бы эквивалентно примерно 1,25 миллиона долларов США, что очень мало как по современным, так и по более ранним стандартам. В результате Подразделение разработало большую часть своего оборудования и программного

обеспечения собственными силами. Эта тенденция сохраняется до наших дней, хотя и с более крупными бюджетами.

Кроме того, с начала 1960-х гг. при администрации президента США Дж. Кеннеди Израилю оказывалась всесторонняя и исключительная поддержка, которая включала в себя и существенную военную составляющую.

Военная помощь со стороны США продолжается и в настоящее время. Израиль имеет статус «основного союзника США вне НАТО» и получает помощь в рамках 3 основных программ: «Военные поставки зарубежным странам» (Foreign Military Sales), «Прямые коммерческие поставки» (Direct Commercial Sales) и «Передача зарубежным государствам неиспользуемой военной техники и имущества» (Excess Defense Articles). В 2001 г. помощь составляла 2,4 млрд долларов США, в 2007 г. – 2,7 млрд. В 2016 г. был заключен меморандум, согласно которому в 2019-2028 гг. Израиль получит от Вашингтона 38 млрд долларов США. Это составляет 3,8 млрд долларов ежегодно без учета дополнительных средств, которые могут быть запрошены через Конгресс.

Также есть основания предполагать наличие у подразделения источников финансирования среди частных компаний и корпораций, основанных выходцами из подразделения и (или) имеющих в руководстве бывших сотрудников подразделения.

Коммерческий и негосударственный секторы

Правительство Израиля активно привлекает к исследованиям и разработкам академические круги и частный сектор. Крупнейшим партнером Подразделения является инновационный парк CyberSpark, а на международном уровне – АНБ (США).

CyberSpark, израильская экосистема киберинноваций в Беер-Шеве, является наиболее заметным израильским проектом государственно-частного партнерства в области киберзащиты. Военные (например, Управление C4I и Подразделение 8200) и правительственные (например, CERT-IL) структуры решили сконцентрировать там ключевые центры кибербезопасности. К реализации проекта был привлечен и частный сектор, в том числе компании Oracle, Lockheed Martin, IBM, Dell, Deutsche Telekom и PayPal. Несмотря на то, что такие экосистемы не являются официальными государственно-частными партнерствами в сфере кибербезопасности, они остаются важной формой сотрудничества. Наконец, платформа для обмена анонимной информацией (CyberNet+) позволяет сотрудничать с частным сектором, получая одновременно и прибыль, и важную информацию.

Кроме того, после окончания службы в Подразделении его бывшие сотрудники часто успешно трудоустраиваются в частные компании в сфере высоких технологий, где применяют и развивают свой опыт. Ветераны в возрасте от 40 до 50 лет входят в состав резервных сил ЦАХАЛа. Таким образом спецслужбы и армия укрепляют и расширяют связи с коммерческими компаниями.

Ветераны Подразделения только в Израиле и США основали более 1000 компаний – от широко известного навигационного сервиса Waze и компании в сфере кибербезопасности Check Point до компании Mirabilis, разработчика мессенджера ICQ.

Количество успешных стартапов, основанных выходцами из Подразделения 8200, составляет 90% от общего числа подобных фирм. Все эти фирмы специализируются в области разработки программного обеспечения и кибербезопасности.

Аффилированные лица и активы

Ключевые лица в настоящее время

В 2021 г. у подразделения сменился командир. Личность действующего командира засекречена.

Асав Кочан (родился в 1971 г.) – командир Подразделения 8200 в 2017-2021 гг. До этого занимал командные должности в ЦАХАЛ и разведывательных организациях. С 2011 г. был заместителем командира Подразделения 8200. При Кочане особый приоритет отдавался развитию кибертехнологий, используемых подразделением, а также активная интеграция с другими подразделениями ЦАХАЛ и улучшение оперативной работы. Во время пребывания Кочана на посту командира подразделения произошел инцидент, связанный со смертью Каба Томера, кадрового офицера ЦАХАЛ, обвиняемого в госизмене. Информация, связанная с инцидентом, засекречена, но ряд открытых источников приписывают Подразделению 8200 непосредственное участие в аресте и, возможно, убийстве Томера.

После ухода из Подразделения 8200 Кочан основал компанию **Sentra**. Ее основная специализация – информационная безопасность в облачной среде.

Нир Ламперт (родился в 1960 г.) – бывший заместитель командира Подразделения 8200, руководитель Ассоциации выпускников 8200 (S.M.2). После отставки был заместителем генерального директора телекоммуникационной компании YES, затем был генеральным директором «10 телеканала» и компании Zap Group (управляет рядом новостных порталов и иных информационных ресурсов). В настоящее время является председателем публичной компании **Mer Industries Ltd**.

Политики и военные руководители, связанные с Подразделением

Среди лиц, тесно связанных с Подразделением 8200, есть бывшие и действующие политические деятели, представители военного руководства страны, а также крупных компаний в области кибербезопасности.

Ицхак Герцог (הרצוג יצחק), род. В 1960 г. – действующий президент государства Израиль, избран на этот пост 2 июня 2021 г. Проходил службу в Подразделении 8200. Занимал посты председателя партии «Авода», лидера оппозиции в Кнессете, министра социального обеспечения. 1 августа 2018 года был избран главой Еврейского агентства «Сохнут».

Известен как сторонник мирного урегулирования палестино-израильского конфликта по принципу «два государства для двух народов». В сентябре 2015 года призывал руководство страны пустить сирийских беженцев в Израиль.

Буки Кармели (Buky Carmeli) – бывший офицер Подразделения 8200, генеральный директор Национального управления кибербезопасности Израиля. Бывший генеральный директор хедж-фонда Sphera Systematic Hedge, входящего в крупнейшую израильскую группу по управлению хедж-фондами Sphera. Бывший начальник управления киберзащиты и защиты технологий Министерства обороны США. Предприниматель и основатель с более чем 30-летним опытом руководства крупными R&D-командами.

Инженер, имеет степень бакалавра в области электроники и вычислительной техники (B.Sc.) Университета Бен-Гуриона. Опубликовал несколько научных статей в области кибербезопасности.

Гади Айзенкот (אייזנקוט גדי), род. в 1960 г. – начальник Генштаба Армии обороны Израиля в 2015-2019 гг. Генерал-лейтенант запаса Армии обороны Израиля, 21-й Начальник Генерального штаба Армии обороны Израиля. Депутат кнессета 25-го созыва в рамках парламентской фракции «Ха-махане ха-мамлахти», министр без портфеля и член малого военного кабинета в Чрезвычайном правительстве национального единства с 12 октября 2023 года.

Биньямин Нетаньяху (נתניהו בנימין), род. в 1949 г. — израильский государственный и политический деятель, нынешний премьер-министр Израиля. Также занимал эту должность с 1996 по 1999 гг. и с 2009 по 2021 гг.

Министр обороны Израиля (2018—2019 гг.), министр юстиции (1996г.), финансов (2003—2005гг., иностранных дел (2002—2003 гг.), строительства (1996—1999гг.), науки культуры и спорта (1996—1997 гг.), связи (2014—2017 гг.), министр диаспоры (2019—2020 гг.) и министр по делам религий Израиля (1996г.).

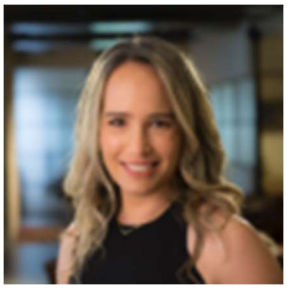
Лидер партии Ликуд (1993—1999 гг., и с 2005 года). Депутат Кнессета (1988—1996 гг., 2005—2009 гг., 2021—2022 гг.). В период с 2005 по 2009 гг. и с 2021 по 2022 гг. — лидер оппозиции в кнессете.

Предприниматели и общественные деятели – выпускники Подразделения

Ариэль Парнес (Ariel Parnes) - соучредитель и исполнительный директор Mitiga, стартапа в области кибербезопасности облачных решений. Он возглавляет группы Mitiga по исследованиям кибербезопасности, центр мониторинга угроз и реагирования на них. Бывший сотрудник Подразделения, ушел в отставку в звании полковника. Был удостоен престижной премии министерства обороны Израиля за прорывные инновации в сфере кибербезопасности.

Гил Азриелант (Gil Azrielant), соучредитель и технический директор Axis Security, отвечает за технологическую стратегию компании и развитие платформы. До прихода в Axis Security был соучредителем и техническим директором Cool Cousin. Карьера

Азриеланта в сфере кибербезопасности началась в Подразделении 8200, где над сложными решениями и и расшифровкой кодов. В Подразделении занимал должности исследователя и руководителя группы.



Шира Шамбан (Shira Shamban), генеральный директор и соучредитель Solvo, исследователь безопасности и технический эксперт в области анализа угроз. Начала свою карьеру в области кибербезопасности в качестве офицера Подразделения 8200. За 13 лет службы в подразделении Шамбан приобрела практический опыт в области кибербезопасности и разведывательных операций, получив диплом инженера в Тель-Авивском университете. После службы занялась инновациями в области кибербезопасности для бизнеса. Выступает в качестве лектора и наставника на таких форумах, как SheCodes и OWASP-WIA.

Авнер Турнянски (Avner Turniansky) – вице-президент по стратегии в Vorpal Ltd, израильском производителе продуктов для РЭР и решений для борьбы с дронами и геолоцирования. Специалист по радиотехнической разведке. Долгое время служил в Подразделении 8200.

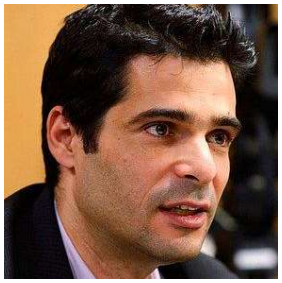
Идан Гур (Idan Gour) – технический директор и соучредитель Astrix Security, корпоративного решения, обеспечивающего взаимосвязь между приложениями. Обладает более чем десятилетним опытом работы в области кибербезопасности в военной и корпоративной среде. Занимал командные должности в Подразделении 8200, позднее был разработчиком программного обеспечения в Deep Instinct.

Чарльз Блаунер (Charles Blauner) – CISO в Team8, венчурной группе в области кибербезопасности, обработки данных и искусственного интеллекта. Более 30 лет работал в сфере информационной безопасности, в основном в сфере финансовых услуг, с 2005 г. занимал руководящие должности в Citigroup с 2005 года. До этого занимал должность CISO в JP Morgan и Deutsche Bank.

Авишай Авиви (Avishai Avivi) – директор по информационной безопасности SafeBreach. Имеет более 30 лет опыта работы в кибербезопасности, ранее служил в Подразделении 8200. Эксперт в области разработки ПО исетевого инжиниринга.

Занимал руководящие должности в таких компаниях, как Palo Alto Networks, Wells Fargo, E*TRADE, Draft Security и др.

Гади Мазор (Gadi Mazor) – технический директор известной израильской краудфандинговой платформы OurCrowd. Ветеран Подразделения 8200. С отличием окончил офицерские курсы ЦАХАЛА с отличием, имеет степени бакалавра и магистра с отличием в области математике и теории вероятностей (проходил обучение в рамках междисциплинарной программы Ади Лаутмана по повышению квалификации в Тель-Авивском университете). Основал и возглавил три стартапа в области распознавания символов и голоса, а также беспроводной связи. Входил в консультативный совет BlackBerry.



Тальмон Марко (Talmon Marco) – израильско-американский предприниматель, сооснователь компании Viber Media. Прошел обязательную подготовку в Подразделении 8200. Служил в ВВС Израиля, был IT-директором Центрального командования. Получил степень бакалавра в области компьютерных наук в Тель-Авивском университете. В 1997 году стал одним из основателей Expand Networks и был президентом этой компании до 2004 года. В 1998 году стал соучредителем iMesh, где был президентом до 2010 года. В 2010–2014 годах был генеральным директором Viber Media. В 2016 году вместе с Игорем Магазинником основал сервис такси Juno.

Авишай Абрахами (Avishai Abrahami) – соучредитель и генеральный директор Wix. Прошел обязательную подготовку в Подразделении 8200, служил в нем с 1990 по 1992 г. В настоящее время является членом совета директоров SodaStream International Ltd. В 2004-2006 гг. – вице-президент по стратегическим альянсам в Arel Communications Software Ltd., частной израильской компании, специализирующейся на коммуникационных технологиях. В 1998 году стал соучредителем Sphera Corporation, частной компании, разрабатывающей программное обеспечение для управления ЦОД. С 1998 по 2000 года занимал в ней должность главного технического директора, с 2000 по 2003 года – вице-президента по продуктовому маркетингу. В 1993 году – стал соучредителем AIT Ltd., частной израильской компании по разработке программного обеспечения, и занимал должность ее технического директора до продажи компании в 1997 году.

Рафаэль Узан (Raphael Ouzan) – создатель приложения для финансовой безопасности под названием BillGuard. Лауреат Президентской премии Израиля в области технологий и инноваций, а также основатель и председателем Israel Tech Challenge. Во время службы в армии узнал о нехватке талантов в технологической индустрии и стал соучредителем некоммерческой организации Israel Tech Challenge. При поддержке Национального кибербюро Израиля, Еврейского агентства, частных спонсоров и корпоративных партнеров, таких как Check Point, Microsoft, PayPal и Intel, организация ищет молодых специалистов на международном уровне и предоставляет им возможность пройти обучение в области Data Science, кибербезопасности и разработки ПО.

Гил Швед (Gil Shwed) – израильский инженер-программист, изобретатель и предприниматель. Соучредитель и генеральный директор Check Point Software Technologies Ltd, одной из крупнейших израильских технологических компаний и одной из крупнейших в мире компаний по кибербезопасности. Член Попечительского совета Тель-Авивского университета, председатель Попечительского Молодежного совета Тель-Авивского университета.

Йоэль Гат (Yoel Gat) – известный эксперт в области спутниковой связи, основатель и генеральный директор компании SatixFy. Один из основателей спутниковых сетей Gilat, основатель нескольких успешных высокотехнологичных компаний, включая Stickspay и Reissat.

Шломо Доврат (Shlomo Dovrat) – израильский предприниматель в области высоких технологий, соучредитель и генеральный партнер Viola Ventures, израильской венчурной компании, под управлением которой находится более 4,5 млрд долларов. Возглавляет израильскую национальную комиссию по реформе образования, известную как комиссия Доврата.

Ключевые активы и связи с другими компаниями

Подразделение 8200 часто называют «кузницей стартапов», поскольку большинство выходцев оттуда, либо создает собственные успешные компании (как правило, в технологической сфере), либо трудоустраивается в крупные корпорации с сильным

международным брендом. В общей сложности выходцы из подразделения основали более 1000 компаний, причем успешными из них оказались более 90%.

Google. В настоящее время в компании работают не менее 99 бывших сотрудников Подразделения 8200. Так, Джонатан Коэн, бывший руководитель группы в подразделении, в настоящее время возглавляет в Google отдел аналитики и обработки данных, а бывший офицер киберразведки Бен Бариах является менеджером работе с партнерами в Лондоне.

Palantir, американская компания – разработчик программного обеспечения для анализа данных. Известно, что в ней некоторое время работал Ори Дэниэл, бывший специалист по техническим операциям в Подразделении 8200, впоследствии также перешедший в Google.

Meta (признана в России экстремистской организацией) – транснациональная холдинговая компания, владеющая, помимо прочего, социальными сетями Facebook и Instagram. Ветеран Подразделения 8200 Эми Палмор входит в Наблюдательный совет Facebook, а ее бывший сослуживец Эяль Кляйн возглавляет отдел обработки данных Facebook Messenger.

Microsoft. Ветеран Подразделения 8200 Эли Цейтлин некоторое время возглавлял в корпорации направление разработки, специализируясь в том числе на вопросах обработки файлов и защите облачных сервисов. Впоследствии перешел в Meta.

NSO Group, израильская компания – разработчик программного обеспечения. Известна как создатель Pegasus – программы для несанкционированной слежки. Считается, что к разработке и распространению Pegasus были причастны бывшие и действующие сотрудники Подразделения 8200.

Toka, израильская компания, с 2018 г. предлагающая «специализированную экосистему решений для государственных и правоохранительных органов, а также служб безопасности». Компания позиционировала себя как поставщика инструментов слежения и контроля для любых устройств с целью борьбы с терроризмом и другими угрозами национальной безопасности в цифровой сфере», а также решений для обеспечения кибербезопасности. Компания официально заявляла, что сотрудничает только с «проверенными» правительствами и организациями. Компания открыто сотрудничает с Министерством обороны Израиля. Один из основателей компании, Ярон Розен, ранее возглавлял одно из крупнейших подразделений ЦАХАЛ по вопросам кибербезопасности. Другой сооснователь компании, Эхуд Барак, ранее возглавлял израильскую военную разведку (АМАН).

NICE Systems, израильская компания – поставщик ИТ-решений для крупного бизнеса, в том числе одного из ведущих мировых антифрод-решений NICE Actimize.

Основана в 1986 г. выходцами из ряда подразделений ЦАХАЛ, включая Подразделение 8200. Изначально создавала решения для военной сферы.

Check Point, американо-израильская компания, крупный поставщик оборудования и ПО, включая решения для кибербезопасности. Один из основателей компании, Гил Швед, является выходцем из Подразделения 8200, где занимался вопросами защиты сетей. Считается, что идея создания компании и ее основных технологий в области безопасности зародилась у Шведа именно во время службы в подразделении.

Выпускниками Подразделения также были основаны такие технологические компании, как Adallom, Argus Cyber Security, Gideon, Onavo, Viber, ZoomInfo и ряд других.

Полный список компаний, основанных выпускниками Подразделения, представлен в Приложении 1.

Ключевые проекты компании (международный охват)

Сотрудничество с ЦРУ и АНБ

В 2016 г. Израиль и США подписали Декларацию о киберзащите, в которой прописано функциональное взаимодействие для израильской и американской групп реагирования на киберцинциденты.

Еще одно партнерство было зафиксировано в Меморандуме о взаимопонимании между США и правительством Израиля по вопросам внутренней безопасности (2008 г.).

В 2009 г. между был подписан Меморандум о сотрудничестве между АНБ и Подразделение 8200. Помимо прочего, он предусматривал согласие АНБ на предоставление Подразделению 8200 различных данных, включая метаданные, голосовые и текстовые данные и т.д.

На конференции Cyber Week в июне 2019 года директор INCD представил список из 36 стран и 13 организаций и компаний, с которыми Израиль наладил международное сотрудничество, но не уточнил, каким образом они сотрудничают.

В 2021 году Объединенное подразделение киберзащиты Армии обороны Израиля, включая Подразделение 8200, и подразделение Пентагона по киберзащите провели совместные учения, включающие подготовку «к различным задачам в области киберзащиты в США».

Предполагается, что в 2022 г. Подразделение 8200 отразило атаку на энергетическую сеть США. На брифинге в Тель-Авивском университете заместитель директора подразделения 8200, известный как «полковник Y», сообщил, что некий противник совершил кибератаку на Израиль и что в ходе отражения атаки также была выявлена попытка атаковать электростанции США.

Наиболее известные операции Подразделения 8200

- Шестидневная война: **перехват телефонных переговоров между президентов Египта Гамалем Абделем Насером и королем Иордании (1967 г.).** В результате удалось сорвать договоренности о поддержке Египта со стороны Иордании, а также об обвинениях в ведении боевых действия на стороне Израиля, которые Иордания должна была выдвинуть Великобритании и США.

- **Перехват телефонных переговоров Ясира Арафата** и террористической группы, захватившей круизный лайнер в Средиземном море (1985 г.).

- **Кибератака на иранские ядерные объекты в Нетензе** с помощью вредоносного ПО Stuxnet (2005-2010 гг.).

- **Выведение из строя сирийских систем ПВО и радиолокационных систем (2007 г.).** Благодаря этому израильские ВВС смогли нанести удар и уничтожить ядерный реактор в провинции Дэйр-эз-Зор.

- **Перехват иранского корабля**, перевозившего через Красное море оружие и технику для ХАМАС (2014 г.). Перехват удалось осуществить благодаря разведданным от Подразделения 8200.

- **Кибератака на ливанскую государственную телекоммуникационную компанию (2017 г.)**

- **Предотвращение теракта ИГИЛ** (организация запрещена в России) на борту гражданского авиалайнера, следовавшего из Австралии в ОАЭ (2018 г.). Теракт **удалось** предотвратить благодаря своевременному перехвату сообщений террористов.

Кибератак и другие операции, приписываемые Подразделению

- Кибератака на палестинские территории и иранские нефтяные объекты с помощью **ВПО Flame (2007-2012 гг.).** Считается, что целью кибератаки был сбор разведданных для дальнейшей атаки с помощью Stuxnet.

- Атака на производителей промышленных систем в Иране, Судане, Венгрии и ряде других стран с помощью сложного **ВПО Duqu (2009-2011 гг.).**

- Кража чувствительной информации и персональных данных у жителей Ливана, Израиля и Палестины с помощью **ВПО Gauss (2011-2012 гг.).**

- Атака с целью кибершпионажа на объекты в Ливане, Кувейте, Катаре, Иране и на палестинских территориях с использованием сложного **ВПО Mini Flame (2012 г.).**

- Кибершпионаж при помощи сложного **ВПО Duqu 2.0.** Атаке подверглись организации, связанные с переговорами по ядерному соглашению между Ираном и группой «5+1».

- **Международный рейс PS752**. 8 января 2020 г. украинский Boeing 737-800, следовавший по маршруту Тегеран – Киев, был сбит Корпусом стражей исламской революции. По одной из версий, катастрофа произошла вследствие кибератаки со стороны Израиля с прямым участием Подразделения 8200, взломавшего иранскую зенитно-ракетную систему.

Социальные инициативы и образовательные проекты

- **Ассоциация выпускников 8200 (S.M.2).** Основана в 1989 г. Среди основных целей – сохранение наследия подразделения, поддержка развития технологий и предпринимательства, технического образования, а также достижение равных возможностей по трудоустройству и карьере для женщин, особенно в высокотехнологичных сферах.

- **Программа «Будущее»**, в рамках которой военнослужащие подразделения ведут уроки в школах 3 раза в неделю. Школьники получают возможность углубленно изучить арабский и персидский языки и пройти начальную военную подготовку.

- **Программа «Магашим»** для старшеклассников, нацеленная на углубленное изучение программирования, разработки ПО и т.д. В рамках программы также проводятся хакатоны и организуются летние образовательные лагеря. Помимо Подразделения 8200, программу также поддерживают ряд министерств, благотворительных фондов и организаций, специализирующихся в сфере ИТ и ИБ.

- **Программа Bridges Unit,** запущенная в апреле 2022 г., предусматривает углубленную подготовку по предметам, связанным с высокими технологиями, для школьников из отдаленных районов и городов.

Деятельность в России и на территории бывшего СССР

Взлом «Лаборатории Касперского»

В 2015 г. Подразделение 8200 с помощью ВПО Duqu 2.0 взломало российскую компанию «Лаборатория Касперского», одного из мировых лидеров в области антивирусного программного обеспечения. В результате расследования якобы выяснилось, «Лаборатория Касперского» предоставляла российским спецслужбам о своих зарубежных клиентах, включая правительственные агентства США. Кампания получила широкую огласку в мировых СМИ. Израиль официально предупредил США о «масштабном российском вторжении», что привело к решению удалить программное обеспечение Kaspersky с правительственных компьютеров.

Программа «Тальпиот»

Программа «Тальпиот» (Talpiot) – это элитная учебная программа Армии обороны Израиля, среди участников которой много иммигрантов из бывшего СССР. США рассматривают программу как один каналов утечек информации об американских технологиях и военных разработках, поскольку считают, что именно через нее происходит внедрение российских спецслужб в американские высокотехнологичные организации и субъекты КИИ.

Приложение 1. Перечень компаний, основанных выходцами из Подразделения 8200

1. Adallom
2. AlphiMAX
3. Altnext
4. Argus Cyber Security
5. Armis
6. Astrix Security
7. AudioCodes
8. Axis Security
9. Bizo
10. Bzigo
11. CardScan
12. Check Point
13. Claroty
14. CloudEndure
15. Cloudinary
16. CommScope
17. Crosswise
18. CTERA Networks
19. CTS Labs
20. CyberArk
21. Cybereason
22. CyCognito
23. Cypago
24. Dig Security
25. Explorium
26. Entitle
27. EZchip
28. Fireblocks
29. Forter
30. FST Biometrics
31. GIDEON
32. Gilat
33. Hub Cyber Security
34. Hunters.Ai
35. Hyperwise Security
36. ICQ
37. IL Ventures
38. Imperva
39. Incapsula
40. Indeni
41. Infinidat
42. Infinipoint
43. IntSights
44. IVIX
45. Lacoon Mobile Security
46. Leadspace
47. LEVL Technologies
48. noname Security
49. Namogoo
50. NICE
51. NSO Group
52. Onavo
53. Opster
54. OverOps
55. Palo Alto Networks
56. PerimeterX
57. PrimeSense
58. Radware
59. Rosh Intelligent Systems
60. Salt Security
61. Secdo
62. Silverfort
63. Solaredge
64. Viber
65. Votiro
66. Verint (дочерняя компания Comverse)
67. Waze
68. Wing Security
69. Wix
70. Wiz
71. XenSource
72. XIV
73. Yonatan Labs
74. ZoomInfo