настоящее время

РОССИЯ

Россиянина Дениса Обрезко подозревают в кибератаках в ЕС и США. Что известно о деле и как он связан с кражей адресов сторонников Навального

Майк Экель

меньше минуты назад

Денис Обрезко работал в ФСБ и Министерстве по чрезвычайным ситуациям РФ

6 ноября 2025 года 35-летний программист **Денис Обрезко** из Самарской области был задержан полицией Таиланда – на основании ордера на арест, выданного на его имя в США. В гостиничном номере Обрезко в курортном городе Пхукет полиция изъяла ноутбук, мобильный телефон и электронный кошелек.

Обрезко был экстрадирован в США, и в июле предстал перед федеральным судом в Бостоне, где проходили предварительные слушания по его делу. Он был обвинен во взломах информационных систем десятка американских компаний и государственных

учреждений. Вину россиянин не признал, в США ему грозит до 10 лет тюремного заключения.

"Господин Обрезко заявил о своей невиновности и намерен активно защищаться в суде как с юридической, так и с фактической точки зрения, – сказал адвокат россиянина Максим Немцев. – Поскольку дело находится на рассмотрении, мы не считаем уместным обсуждать факты в прессе".

ФСБ и база сторонников Навального

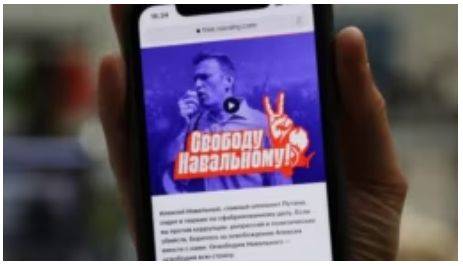
Согласно информации в аккаунте в российской социальной сети "ВКонтакте", Обрезко окончил Московский технический университет имени Баумана. Этот вуз называют "кузницей" современных российских хакеров, связанных с государством.

Как сообщает Reuters, сначала Обрезко работал в "Лаборатории Касперского", компании-разработчике российского антивирусного программного обеспечения (она находится под санкциями в США из-за подозрений в связях с Кремлем и российскими спецслужбами). В 2021 году он выступал в качестве приглашенного докладчика на мероприятии, организованном Московским техническим университетом связи и информатики. Тогда его представили как заместителя директора информационно-аналитического центра (ИАЦ) МЧС России.

Денис Обрезко (второй справа) в 2021 году на конференции в Московском техническом университете связи и информатики

При этом, согласно документам ФБР, обнародованным для процедуры экстрадиции россиянина в США, с 2012 по 2017 год Обрезко работал в ФСБ. Но какие именно функции он там выполнял, неясно.

Согласно документам американского суда, на момент задержания в Таиланде Обрезко был заместителем директора компании "ЮТЕК", к которой присоединился в 2023 году. Эта компания, как выяснили журналисты Настоящего Времени в 2021 году, была связана с кражей в России базы имейлов, которые сторонники оппозиционера Алексея Навального использовали для регистрации на сайте freenavalny.com. С "ЮТЕК" был связан бизнесмен Михаил Дудин, который, по имеющимся к расследователей данным, сотрудничал с бывшим сотрудником ФСБ в Самарской области Павлом Селезневым:



СМОТРИТЕ ТАКЖЕ:
Операция Navalnyfail. Куда ведут цифровые следы распространителей почтовой базы сторонников Навального

По цифровым следам тогда удалось установить, с каких адресов электронной почты рассылались угрозы сторонникам Навального, чьи электронные адреса были в украденной базе данных. Домены, с которых это делалось, как выяснилось, были связаны с Дудиным, а одна из компаний Дудина называлась ООО "ЮТЕК-НН". Она позиционирует себя как компанию, использующую "передовые технологии, инновационные концепции и креативный дизайн". Фирма имела в том числе лицензию на продажу специализированного технического оборудования, предназначенного для скрытого сбора информации: такая лицензия обычно выдается ФСБ.

Хакерская атака в Нидерландах

Обрезко связывают также с хакерской атакой в Нидерландах. В сентябре 2024 года голландские эксперты по кибербезопасности обнаружили, что кто-то проник в компьютерные системы Национальной полиции Нидерландов и получил доступ к электронной почте одного из сотрудников. Злоумышленник или группа злоумышленников использовали украденный файл cookie (фрагмент данных, который временно сохраняют веб-браузеры на устройстве пользователя) для доступа к электронной адресной книге.

Использовав этой файл, хакеры получили доступ ко всем контактам в электронной почте сотрудника полиции Нидерландов, а возможно и к контактам всех 64 тысяч сотрудников ведомства. Также они потенциально могли получить именах источников или информаторов, с которыми работает полиция.

"Этот случай вызвал резонанс в СМИ, и значительное беспокойство законодателей, сотрудников спецслужб и широкой общественности Нидерландов, – говорит Барт ван ден Берг, бывший ведущий аналитик разведки и специалист по кризисному управлению в Национальном центре кибербезопасности Нидерландов. – Это был чувствительный вопрос".

СМОТРИТЕ ТАКЖЕ:

В Нидерландах за шпионаж в пользу России задержали двоих подростков: они пытались перехватить интернет-сигнал из учреждений

При этом в июне и июле 2024 года, еще до того, как стало известно о хакерской атаке на полицию Нидерландов, ФБР получило уведомление из частного сектора в США – предположительно, речь шла о компании Microsoft – о том, что объектами схожих хакерских атак стали американские и европейские компании, а также государственные учреждения в разных странах. Согласно этим документам, сотрудники компании "ЮТЕК" скопировали электронные письма "различных правительственных ведомств по всей Европе, являющихся партнерами НАТО, а также других организаций, поддерживающих сопротивление Украины российскому военному вторжению". "ЮТЕК "проводил эти операции по кибершпионажу по поручению российского правительства", – говорится в документах.

Следователи ФБР США отследили путь поддельных электронных писем, которые использовались в этих хакерских атаках, к ряду адресов скомпрометированной электронной почты. Затем они обнаружили связь ряда транзакций, совершенных в 2024 и 2025 годах, с криптовалютой. Одна из транзакций вела к интернет-провайдеру в Самаре. В конечном итоге следователи заявили, что один из адресов электронной почты, использовавшийся для транзакций с криптовалютой, был напрямую связан с одним почтовым ящиком Google: он был зарегистрирован на настоящее имя Дениса Обрезко.

Этот же почтовый ящик Google использовался для регистрации нескольких аккаунтов в социальных сетях, в том числе в X и Instagram, а также учетной записи в PayPal, где был указан тот же номер мобильного телефона, который был идентифицирован как принадлежащий Обрезко. Там же была указана и дата его рождения. Тот же логин и фотография использовались еще для нескольких аккаунтов в социальных сетях, в том числе в Instagram.

27 мая 2025 года правительство Нидерландов публично обозначило хакеров, взломавших системы Национальной полиции, как "российскую хакерскую группу,

поддерживаемую государством" и назвало ее Laundry Bear – по аналогии с другими связанными с Россией хакерскими "медведями" ("bear"):

СМОТРИТЕ ТАКЖЕ:

- Российские хакеры взломали систему Республиканской партии США – Bloomberg
- Возвращение "Уютного медведя": российские спецслужбы подозревают в крупнейшей кибератаке на ведомства США
- Spiegel сообщил о хакерах из России, которые в 2015 году получили доступ к компьютеру Меркель

"Нидерланды впервые стали жертвой целенаправленного киберпреступления со стороны группы, поддерживаемой Россией", – сообщила в своем отчете военная разведка Нидерландов. По их словам, хакерская группа, позже названная Laundry Bear, "продемонстрировала немалую эффективность".

В отчете Microsoft, опубликованном в тот же день, эта хакерская группа была названа Void Blizzard. Но в тот момент ни в отчете Нидерландов, ни в отчете Microsoft не были указаны конкретные лица или даже конкретные компании, причастные ко взлому.

Зато всего через несколько часов после публикации отчета Microsoft, согласно данным ФБР, Обрезко отправил со своей почты электронное письмо некоему "Итану Ханту", предложив встретиться позже в тот же день. "Итана Ханта" (видимо, в честь главного героя фильмов "Миссия невыполнима") ФБР США называет "неустановленным соучастником" группы. При этом расследователи Настоящего Времени в материале о краже базы имейлов сторонников Навального смогли его деанонимизировать: это упоминавшийся выше Михаил Дудин. Так он обозначен в записных книжках некоторых людей в приложении GetContact.

Еще два варианта записи этого контакта, "Михаил Юдин От Лугового Биткоин" и "Михил Админ Прзидент" указывает на возможную связь Дудина с администрацией президента России и депутатом Андреем Луговым, также выходцем из ФСБ, но эта связь не подтверждена.

"Цепочка доказательств, основанная на ряде мелких оперативных ошибок"

По словам Александра Лесли, старшего советника американской организации по кибероборонe Recorded Future, Обрезко допустил ошибку, повторно использовав одно и то же имя пользователя и свой российский номер мобильного телефона для разных учетных записей – электронной почты и социальных сетей.

"Похоже, ФБР вычислило его благодаря одной катастрофической ошибке. Следователи постепенно собрали цепочку взаимодополняющих доказательств, основанную на ряде мелких оперативных ошибок, – объясняет Лесли, как работали следователи. – Хакер может быть чрезвычайно эффективен в получении доступа, краже информации и уклонении от обнаружения, но при этом менее эффективен в сокрытии своей личности в ходе длительного контрразведывательного расследования".

Чем именно занимался Обрезко в Таиланде, куда он приехал с ноутбуком, неясно, но этот выезд за границу также стал его большой ошибкой.

Обрезко проявил неосторожность, считает ван ден Берг: "О чем он думал, отправляясь в Таиланд? Когда находишься за пределами России, есть риск быть арестованным. Видимо, что-то пошло не так: или он недооценил западные спецслужбы или переоценил свою защиту [со стороны российского государства]".

Арест и экстрадиция российских хакеров на основании ордеров США в разных странах мира раньше были обычным явлением. Москва публично выражала несогласие с этими действиями, и даже обвинял[а] США в "охоте" на российских граждан.

- В октябре 2016 года россиянин Евгений Никулин был арестован во время попытки въехать в Чехию, а затем экстрадирован в США. Разыскиваемый за организацию взлома социальной сети LinkedIn, Никулин в 2020 году был приговорен к семи годам лишения свободы в США, а три года спустя депортирован в Россию. Телеканал Настоящее Время рассказывал о его деле:

СМОТРИТЕ ТАКЖЕ:

Арестованного в Праге россиянина обвинили во взломе LinkedIn, Dropbox и Formspring

- В марте 2021года в Швейцарии был арестован Владислав Клюшин, IT-предприниматель, связанный с Кремлем. Ему предъявили обвинение в причастности к схеме незаконной торговли акциями с использованием взлома чужих компьютеров. Американские власти установили его связь с офицером российской военной разведки, который обвинен во взломе компьютеров Демократической партии в 2016 году. Приговоренный к девяти годам лишения свободы, Клюшин был освобожден в 2024 году и вернулся в Россию в рамках крупного обмена заключенными, в который были включены в том числе американцы, содержавшиеся в российских тюрьмах.

СМОТРИТЕ ТАКЖЕ:

Эксклюзив: хакеры Клюшин и Селезнев, вернувшиеся в Россию в рамках обмена заключенными, открыли новые бизнесы

По мнению экспертов и следователей, проблемы с российской киберпреступностью обусловлены размытостью границ между преступными группировками и спецслужбами, такими как ФСБ и ГРУ.

"Для западного мышления типично представление, что между сферой государства и сферой преступности существует четкое разграничение. Но в России это не так", – подчеркивает ван ден Берг.

В случае с кибератакой на Нидерланды, поясняет ван ден Берг, киберпреступник мог, например, попытаться вымогать деньги у жертвы, чью электронную почту он получил, шантажировать ее или попытаться совершить какую-либо коммерческую сделку. Но также он мог работать и по заказу ФСБ.

"Мы имеем дело с преступным нападением или с бизнес-моделью? Поскольку суть бизнес-модели неясна, можно задаться вопросом: кто платит этому человеку? – говорит эксперт. – Он продает похищенные данные (российскому) государству или работает непосредственно на него? Если окажется, что дело обстоит именно так, то это означает, что государство в той или иной степени к этому причастно".

МАТЕРИАЛ ИЗ РАЗДЕЛОВ:

В деталях | Видео и статьи | Россия | Европа | Америка | Актуальное