**16 мая 2022 г.**

# РУКОВОДСТВО В ОТНОШЕНИИ СПЕЦИАЛИСТОВ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КОРЕЙСКОЙ НАРОДНОЙ ДЕМОКРАТИЧЕСКОЙ РЕСПУБЛИКИ

Государственный департамент США, Министерство финансов США и Федеральное бюро расследований (ФБР) публикуют данное руководство для международного сообщества, частного сектора и общественности с целью предупреждения о попытках специалистов в сфере информационных технологий (ИТ) Корейской Народно-Демократической Республики (КНДР), также известной как Северная Корея, устроиться на работу, выдавая себя за граждан других стран. Для физических и юридических лиц, осуществляющих или поддерживающих деятельность, связанную с привлечением специалистов в сфере ИТ из КНДР, и соответствующие финансовые операции, существуют репутационные риски и возможность юридических последствий, включая введение санкций со стороны властей США и Организации Объединенных Наций (ООН).

В нарушение санкций США и ООН КНДР направляет тысячи высококвалифицированных ИТ-специалистов по всему миру для получения доходов, которые способствуют реализации ее программ по созданию оружия массового поражения (ОМП) и баллистических ракет. Эти ИТ-специалисты используют высокий спрос на специальные навыки в сфере ИТ, такие как разработка программного обеспечения и мобильных приложений, чтобы заключить контракты в качестве фрилансеров с клиентами по всему миру, в том числе в Северной Америке, Европе и Восточной Азии. Во многих случаях ИТ-специалисты из КНДР представляются работающими удаленно специалистами из США и/или специалистами, не являющимися гражданами Северной Кореи. Эти работники могут дополнительно скрывать свою личность и/или местонахождение, передавая работу на субподряд специалистам не из Северной Кореи. Хотя ИТ-специалисты из КНДР обычно осуществляют ИТ-разработки, не связанные с вредоносной деятельностью, они используют привилегированный доступ, полученный в качестве подрядчиков, для осуществления вредоносных взломов компьютерных сетей по заданию КНДР. Кроме того, вероятны случаи, когда работники подвергаются принудительному труду.

Данное сообщение содержит подробную информацию о деятельности ИТ-специалистов из КНДР, индикаторы риска для компаний, нанимающих фриланс-разработчиков и использующих

платежные платформы, которые позволят выявить ИТ-специалистов из КНДР, а также общие меры снижения риска, которые помогут компаниям усилить защиту от найма ИТ-специалистов из КНДР или содействия их деятельности. В приложении представлена дополнительная информация по ИТ-специалистам из КНДР на основании отчетов, подготовленных панелью экспертов Комитета по санкциям Совета Безопасности ООН в отношении Северной Кореи на основании резолюции 1718. ФБР призывает американские компании сообщать о подозрительной деятельности, включая любые подозрения в деятельности ИТ-специалистов из КНДР, в местные подразделения.

## СПЕЦИАЛИСТЫ В СФЕРЕ ИТ ИЗ КНДР: ОБЩИЕ СВЕДЕНИЯ

ИТ-специалисты из КНДР обеспечивают важнейший поток доходов, который помогает финансировать наиболее приоритетные направления экономики и безопасности режима КНДР, такие как программа разработки оружия. Лидер КНДР Ким Чен Ын признает важность ИТ-специалистов как значительного источника иностранной валюты и доходов и поддерживает их деятельность.

Тысячи ИТ-специалистов из КНДР работают как за рубежом, так и в КНДР, получая доход, который перечисляется обратно правительству Северной Кореи. ИТ-специалисты из КНДР находятся в основном в Китайской Народной Республике (КНР) и России, меньшая численность — в Африке и Юго-Восточной Азии. Эти ИТ-специалисты часто пользуются услугами знакомых, проживающих за рубежом, чтобы получить работу в качестве внештатных специалистов и напрямую взаимодействовать с клиентами.

Все ИТ-специалисты из КНДР зарабатывают деньги на поддержку режима северокорейского лидера Ким Чен Ына. Подавляющее большинство из них подконтрольны и работают от имени организаций, непосредственно участвующих в запрещенных ООН программах КНДР по созданию ОМП и баллистических ракет, а также в секторах разработки и торговли современным обычным оружием. В результате доходы, полученные от этих ИТ-специалистов из КНДР, используются КНДР для развития своих программ по созданию ОМП и баллистических ракет, в нарушение санкций США и ООН. Многие из этих организаций были включены в список санкций ООН и США. В число организаций, направляющих ИТ-специалистов из КНДР, входят:

- **Главное бюро 313 при Департаменте военной промышленности (ДВП)**, которое контролирует исследования, разработки и производство оружия КНДР, включая ядерное оружие, баллистические ракеты и другую военную технику. ДВП подчиняется Центральному комитету Трудовой партии Кореи и через Главное бюро 313 направляет большую часть ИТ-специалистов из КНДР за рубеж. Вся собственность и имущественные права Трудовой партии Кореи заблокированы в соответствии с Исполнительным распоряжением 13722.

- **Министерство атомной энергетики —** критически важный игрок в разработке ядерного оружия в КНДР, отвечающий за повседневную работу программы ядерного оружия КНДР. Министерство атомной энергетики включено в список на основании Исполнительного распоряжения 13382.

- Военные структуры, подчиняющиеся **Министерству обороны и Корейской народной армии.** Корейская народная армия включена в список лиц особых категорий и запрещенных лиц и заблокированного имущества.

- Менее известные организации, такие как **Управление внешней торговли Комиссии по образованию КНДР** и **Пхеньянское бюро информационных технологий при Департаменте науки и образования Центрального комитета.** Вся собственность и имущественные права правительства КНДР заблокированы в соответствии с Исполнительным распоряжением 13722.

Зарубежный ИТ-специалист из КНДР зарабатывает как минимум в десять раз больше, чем обычный северокорейский рабочий, работающий на заводе или на строительном объекте за рубежом. Отдельные ИТ-специалисты из КНДР могут в некоторых случая зарабатывать более 300 000 долларов США в год, а команды ИТ-специалистов могут совместно зарабатывать более 3 миллионов долларов США в год. Значительный процент их валового дохода идет на поддержку приоритетов режима КНДР, включая его программу по созданию ОМП.

ИТ-компании из КНДР и их сотрудники обычно занимаются широким спектром разработок в сфере ИТ различной степени сложности, например:

- мобильные приложения и веб-приложения,
- создание бирж виртуальных валют и цифровых валют,
- общая поддержка в сфере ИТ,
- графическая анимация,
- программы азартных игр онлайн,
- игры для мобильных устройств,
- приложения для знакомств,
- приложения, связанные с искусственным интеллектом,
- разработки аппаратно-программного обеспечения,
- создание программ виртуальной реальности и дополненной реальности,
- программное обеспечение для распознавания лиц и биометрических данных и
- разработка и управление базами данных.

Приложения и программное обеспечение, разрабатываемые ИТ-специалистами из КНДР, относятся к различным отраслям, включая, в числе прочего, сферы бизнеса, криптовалют, здравоохранения и фитнеса, социальных сетей, спорта, развлечений и образа жизни. ИТ-

специалисты из КНДР часто берут проекты, связанные с виртуальными валютами. Некоторые ИТ-специалисты из КНДР разрабатывали биржи виртуальных валют или создавали аналитические инструменты и приложения для торговцев виртуальными валютами и сами продвигали свои продукты на рынке.

В течение многих десятилетий КНДР подчеркивала важность образования в области математики и естественных наук для своих граждан. Фокус на развитии науки и технологий, который исторически был приоритетом для режима Ким Чен Ына, отражается в инвестировании ресурсов и персонала в соответствующие области исследований. Сегодняшнее образование в сфере компьютерных и информационных технологий в КНДР было основано на этом стремлении к прогрессу и привело к созданию интегрированной учебной программы, скоординированной с Трудовой партией, исследовательскими центрами и вооруженными силами.

- В последние годы режим Ким Чен Ына уделяет повышенное внимание образованию и подготовке по предметам, связанным с ИТ, и разрабатывает сильные программы по получению степени в области ИТ в нескольких ведущих учебных заведениях КНДР, в частности, в Университете имени Ким Ир Сена, Политехническом университете имени Ким Чхэка и Пхеньянском университете науки и технологии. Только в этих ведущих университетах предметы, связанные с информационно-коммуникационными технологиями, изучают около 30 000 студентов.

- Согласно данным на 2019 год в 37 университетах было создано 85 программ, предлагающих курсы по передовым направлениям в области естественных наук, технологий, инжиниринга и математики (STEM), включая информационную безопасность, а в каждой провинции было создано как минимум по одной новой средней школе для перспективных учащихся.

- Система образования в КНДР отличается высокой конкуренцией, и на элитные научно-технологические программы принимаются только лучшие студенты. Отбор учащихся осуществляется в молодом возрасте из таких средних школ, как Kumsong Academy и Kumsong Middle School Number 1.

- ИТ-специалисты из КНДР проходят дополнительное обучение за рубежом и внутри страны, часто через расположенные в КНДР региональные исследовательские ИТ-центры для дальнейшего совершенствования своих навыков. Исторически ИТ-специалисты из КНДР проходят обучение в Восточной Африке, Юго-Восточной Азии и Южной Азии и благодаря этому существенно повышают свой уровень.

## КАК ДЕЙСТВУЮТ ИТ-СПЕЦИАЛИСТЫ ИЗ КНДР

ИТ-специалисты из КНДР стараются получить контракты в качестве фрилансеров от работодателей, расположенных в более богатых странах, в том числе в Северной Америке, Европе и Восточной Азии. Во многих случаях ИТ-специалисты из КНДР представляются работающими удаленно специалистами из Южной Кореи, Китая, Японии, Восточной Европы и США.

В некоторых случаях ИТ-специалисты из КНДР дополнительно скрывают свою личность, заключая соглашения со сторонними субподрядчиками. Эти субподрядчики — фрилансеры из других стран, которые выполняют контракты для ИТ-специалистов из КНДР. ИТ-менеджеры из КНДР также нанимают собственные команды ИТ-специалистов, не являющихся гражданами КНДР, которые обычно не знают о реальной личности своего северокорейского работодателя или о том, что их работодателем является компания из КНДР. ИТ-менеджеры из КНДР используют таких подрядчиков для закупок программного обеспечения и взаимодействия с клиентами в ситуациях, в которых в противном случае вскрылось бы взаимодействие с ИТ-специалистом из КНДР.

Хотя ИТ-специалисты из КНДР обычно выполняют работы, не связанные с вредоносной деятельностью, они используют привилегированный доступ, полученный в качестве подрядчиков, для осуществления вредоносных взломов компьютерных сетей по заданию КНДР. Некоторые ИТ-специалисты из КНДР, находящиеся за рубежом, оказывают логистическую поддержку киберпреступникам из КНДР, хотя сами ИТ-специалисты вряд ли участвуют в злонамеренной кибердеятельности. ИТ-специалисты из КНДР могут делиться доступом к виртуальной инфраструктуре, способствовать продаже данных, украденных кибер-преступниками из КНДР, или помогать КНДР в отмывании доходов, полученных преступным путем, и переводах виртуальной валюты.

ИТ-специалисты из КНДР также оказывают помощь должностным лицам КНДР в приобретении предметов, связанных с ОМП и баллистическими ракетами, для запрещенных оружейных программ КНДР.

Есть примеры, когда эти специалисты становились жертвами торговли людьми, включая принудительный труд.  По достоверным данным, многие работники из КНДР, находящиеся за рубежом, имеют увеличенный рабочий день и находятся под постоянным пристальным наблюдением со стороны агентов службы безопасности северокорейского правительства, проживают в небезопасных и антисанитарных условиях и практически не имеют свободы передвижения.  Правительство Северной Кореи удерживает до 90 процентов заработной платы работающих за рубежом сотрудников, что приносит ему ежегодный доход в сотни миллионов долларов.

## *Специалисты в сфере ИТ из КНДР: навыки и платформы*

Команды ИТ-специалистов из КНДР чаще всего получают работу за рубежом в качестве фрилансеров через различные онлайн-платформы. Компании используют эти платформы для размещения объявлений о контрактах на проекты, на которые могут претендовать внештатные ИТ-разработчики. Реже ИТ-команды из КНДР находят местных граждан, не являющихся гражданами КНДР, для работы в качестве номинальных руководителей компаний, которые на самом деле контролируются северокорейцами. Также известны случаи, когда ИТ-команды из КНДР по документам представлены как сотрудники легальной местной компании, но ведут свой бизнес независимо, и в обмен на сокрытие своего северокорейского происхождения выплачивают иностранной компании вознаграждение. В ИТ-команды из КНДР часто входят сотрудники, хорошо владеющие иностранным языком, например английским или китайским.

ИТ-специалисты из КНДР используют широкий спектр основных и специфических для ИТ-индустрии платформ для поиска фрилансеров, инструменты и платформы для разработки программного обеспечения, приложения для обмена сообщениями, социальные сети и сайты для получения контрактов на выполнение разработок для компаний по всему миру, а также используют ряд цифровых платежных платформ и сайтов для получения гонораров за свою работу. ИТ-специалисты из КНДР используют биржи виртуальных валют и торговые платформы для управления цифровыми платежами, которые они получают за работу в качестве подрядчиков, а также для отмывания и перемещения полученных средств.

## *Специалисты в сфере ИТ из КНДР: сокрытие личности*

ИТ-специалисты из КНДР намеренно скрывают в Интернете свою личность, местонахождение и гражданство, часто используя в качестве псевдонимов некорейские имена. Они также будут использовать виртуальные частные сети (VPN), виртуальные выделенные серверы (VPS) или IP-адреса третьих стран, чтобы создать впечатление, что они подключаются к Интернету из не вызывающих подозрение мест, и снизить вероятность проверки их местонахождения или связи с КНДР. ИТ-специалисты из КНДР обычно полагаются на анонимность удаленной работы, используют прокси-серверы для создания учетных записей, предпочитают использовать посредников и общаться через текстовые чаты вместо видеозвонков.

ИТ-специалисты из КНДР используют учетные записи-посредники, чтобы участвовать и побеждать в тендерах, выполнять работы и получать гонорары за проекты на фриланс-платформах для разработчиков программного обеспечения. Эти учетные записи-посредники принадлежат третьим лицам, некоторые из которых продают свои личные данные и информацию об учетной записи ИТ-специалистам из КНДР. В некоторых случаях ИТ-специалисты из КНДР выплачивают этим лицам вознаграждение за использование их легитимных учетных записей на платформе. ИТ-специалисты из КНДР могут заполнять профили на фриланс-платформах, указывая связи с реальными компаниями и опыт работы посредника.

Периодически ИТ-специалисты из КНДР связываются с фрилансерами из других стран на платформах, предлагая сотрудничество на проектах по разработке ПО. ИТ-специалист из КНДР использует эти деловые отношения для получения доступа к новым контрактам и счетам в виртуальной валюте, используемым для выполнения работы в сфере ИТ через американскую или европейскую виртуальную инфраструктуру, таким образом обходя меры безопасности, предназначенные для предотвращения мошеннического использования. Создавая учетные записи с помощью других фрилансеров, ИТ-специалисты из КНДР могут выдавать себя за граждан третьих стран, которым нужны удостоверения личности и аккаунты из США и стран Запада на фриланс-платформах, чтобы заработать больше денег.

Сокрытие своего реального местонахождения позволяет ИТ-специалистам из КНДР нарушать условия соглашений об обслуживании онлайн-платформ и сервисов, используемых ими для своей деятельности. В рамках своей деятельности ИТ-специалисты из КНДР также могут использовать отдельные устройства для каждой учетной записи, особенно для банковских услуг, чтобы избежать обнаружения в рамках мер по предотвращению мошенничества, соблюдению санкций и борьбе с отмыванием доходов, полученных преступным путем.

ИТ-специалисты из КНДР регулярно используют поддельные, измененные или фальсифицированные документы, включая документы, удостоверяющие личность, и поддельные подписи, либо сделанные ими самостоятельно с помощью специальных программ, таких как Photoshop, либо купленные у компаний, предоставляющих такие услуги, при этом сочетая собственную или предоставленную ИТ-специалистом фотографию с идентификационной информацией реального человека. ИТ-специалисты из КНДР часто используют следующие поддельные документы:

- водительские права,
- карты социального страхования,
- паспорта,
- национальные удостоверения личности,
- карты иностранцев-резидентов,
- аттестаты о среднем образовании и дипломы университетов,
- рабочие визы и
- кредитные карты, банковские выписки и счета за коммунальные услуги.

В некоторых случаях эти идентификационные данные были украдены, а в других — ИТ-специалисты из КНДР просят гражданина другой страны создать учетную запись, используя его личную информацию или информацию, к которой он имеет доступ, после чего контроль над учетной записью передается ИТ-специалистам из КНДР за вознаграждение. Это позволяет ИТ-специалисту из КНДР скрывать свою личность при участии в тендерах и выполнении фриланс-проектов для клиентов через Интернет, используя инфраструктуру реального владельца учетной записи с помощью удаленного доступа к рабочему столу. Каждый ИТ-специалист часто

использует несколько идентификационных данных и учетных записей, которые также могут совместно использоваться сотрудниками из одной команды. Эти учетные записи и идентификационные данные принадлежат странам всего мира.

ИТ-специалисты из КНДР могут красть информацию о счетах клиентов американских или международных банков, чтобы подтвердить свою личность на фриланс-платформах, у провайдеров платежей и компаний, нанимающих ИТ-специалистов из КНДР. По крайней мере, в одном случае ИТ-специалисты из КНДР подделывали чеки, используя украденную информацию о банковских счетах. Учетные записи-посредники и резюме ИТ-специалистов из КНДР часто содержат фальсифицированную, но реалистичную и подробную информацию об образовании и опыте работы, включая ложные контактные данные учебных заведений и предыдущих работодателей.

ИТ-специалисты из КНДР могут также заполнять разделы об опыте работы в своих онлайн-профилях разработчиков названиями малых или средних западных компаний, чтобы при участии в тендерах на проекты выглядеть как специалисты из Америки или Европы с хорошей репутацией. Они могут использовать имена реальных сотрудников и адреса электронной почты, которые выглядят похожими на реальный домен западной компании.

ИТ-специалисты из КНДР дополнительно подделывают договоры на выполнение работ, счета, контактные данные для связи с клиентами и другие документы для использования на фриланс-платформах, чаще всего для того, чтобы соблюсти требования по проверке клиентов и борьбе с отмыванием доходов, полученных преступным путем, (KYC/AML) или аналогичные процедуры, которые платформы применяют для обеспечения легитимности деятельности пользователей. Эти поддельные документы могут содержать минимальную контактную информацию, чтобы не допустить проверки.

ИТ-специалисты из КНДР могут также пытаться скрыть свое гражданство, представляясь гражданами Южной Кореи или просто «корейцами».

Известны случаи, когда ИТ-специалисты из КНДР, осуществляющие сотрудничество в качестве фрилансеров с ничего не подозревающей об их происхождении компанией, впоследствии рекомендовали ей других ИТ-подрядчиков из КНДР.

### *Резюме ИТ-специалиста из КНДР*

ИТ-специалисты из КНДР демонстрируют навыки разработки систем и программ, систем управления базами данных, использования широкого спектра распространенных языков, интегрированных систем, инструментов и облачных ресурсов. Эти навыки часто включают хорошее владение несколькими языками кодирования и разметки.  Большинство проектов ИТ-специалистов из КНДР связаны с разработкой мобильных и веб-приложений.  ИТ-специалисты из КНДР также используют платформы для совместной работы и услуги хостинга для

управления данными и рабочими процессами. Эти специалисты часто сообщают об опыте работы с различными базами данных и знакомы с облачными и аналитическими продуктами и услугами крупных поставщиков. Кроме того, ИТ-специалисты из КНДР используют в своей работе платформы цифровых платежей и электронной коммерции.

Чтобы повысить доверие к своим фальсифицированным личностям разработчиков-фрилансеров, ИТ-специалисты из КНДР создают сайты-портфолио, как правило, простые по дизайну. Эти виртуальные портфолио представляют достижения специалистов в сфере ИТ из КНДР и часто связаны с их онлайн-учетными записями разработчиков-фрилансеров. Информация на этих сайтах, включая контактную информацию и местонахождение, а также историю работы и образование, скорее всего, является ложной.

## ИНДИКАТОРЫ РИСКА

***Компании, являющиеся владельцами платформ для фрилансеров и платежных платформ, должны быть осведомлены о следующих действиях, которые могут быть признаками присутствия ИТ-специалистов из КНДР и использования ими этих платформ.***

- множественные входы в одну учетную запись с различных IP-адресов за относительно короткий период времени, особенно если IP-адреса связаны с разными странами;
- Разработчики входят в несколько учетных записей на одной платформе с одного IP-адреса.
- Разработчики не выходят из своих учетных записей один или нескольких дней подряд.
- Для доступа к учетной записи используется порт маршрутизатора или другие технические конфигурации, связанные с применением программного обеспечения для совместного доступа к удаленному рабочему столу, например порт 3389, особенно если использование такого программного обеспечения не является стандартной практикой компании.
- Учетные записи разработчиков используют мошенническую учетную запись клиента для повышения рейтинга разработчика, но при этом и учетная запись клиента, и учетные записи разработчиков используют один и тот же счет PayPal для перевода/вывода денег (платя себе своими собственными деньгами).
- Часто используются шаблоны документов для подачи тендерных заявок и осуществления коммуникаций на проекте, особенно одни и те же шаблоны с разных учетных записей разработчиков.
- Несколько учетных записей разработчиков получают высокие оценки от одного клиента за короткий период, особенно если для создания учетных записей разработчиков и/или клиента использовалась схожая или идентичная документация.
- Чрезмерно активное участие в тендерах по проектам и низкое количество принятых предложений по проектам по сравнению с количеством проектов, в отношении которых разработчик делал предложения.
- Частые переводы денег через платежные платформы, особенно на банковские счета в КНР, которые иногда направляются через одну или несколько компаний для маскировки конечного назначения средств.

***Компании, осуществляющие наем разработчиков-фрилансеров, должны быть осведомлены о следующих действиях, которые могут быть признаками присутствия ИТ-специалистов из КНДР.***

- Если учетная запись разработчика на фриланс-платформе для разработчиков программного обеспечения или платежной платформе была закрыта или работник обращается к работодателю с просьбой использовать другую учетную запись, особенно если она зарегистрирована на другое имя.

- Использование цифровых платежных сервисов, особенно связанных с КНР.

- Расхождения в написании имени, сведениях о гражданстве, месте работы, контактной информации, сведениях об образовании, опыте работы и других данных в профилях разработчиков на фриланс-платформах, профилях в социальных сетях, на внешних сайтах-портфолио, в профилях платежных платформ, а также несоответствие оценочному местоположению и часовому поясу.

- Необычно простые сайты-портфолио, профили в социальных сетях или профили разработчиков.

- Получение прямых сообщений или холодных звонков от лиц, выдающих себя за руководителей высшего звена компаний, занимающихся разработкой программного обеспечения, с предложением услуг или рекламой профессиональных качеств.

- Запросы на осуществление общения с клиентами и потенциальными клиентами на отдельной платформе, отличной от исходного сайта фриланс-платформы, на котором клиент нашел ИТ-специалиста.

- Работодатель предлагает отправить разработчику документы или необходимое для работы оборудование, например ноутбук, а разработчик просит отправить документы по адресу, отличному от указанного в документах, удостоверяющих его личность. Проявите особую настороженность, если разработчик заявляет, что не может получать отправления по адресу, указанному в его идентификационных документах.

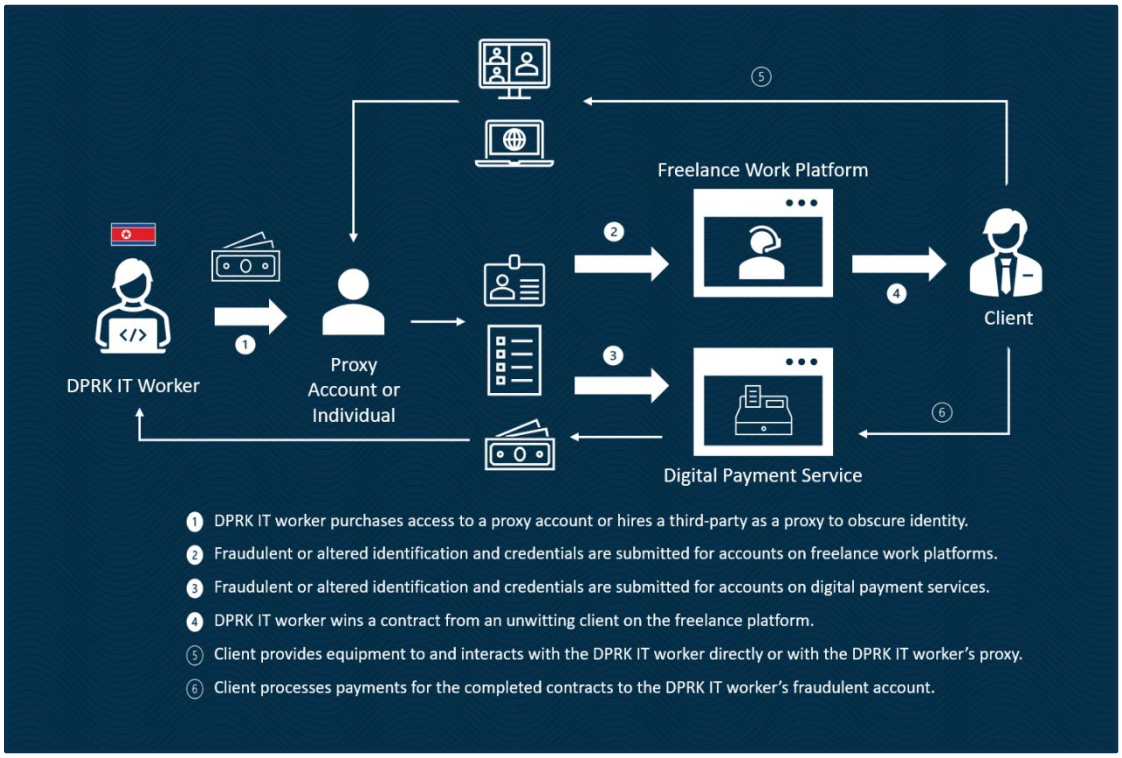
- Просьбы осуществлять оплату в виртуальной валюте с целью обойти меры идентификации клиентов/противодействия отмыванию доходов, полученных преступным путем, и избежать использования официальной финансовой системы.

- Запросы платежей по контрактам до достижения ключевых этапов или проведения контрольных встреч.

- Невозможность ведения дел в установленные рабочие часы.

- Некорректная или меняющаяся контактная информация, особенно номера телефонов и адрес электронной почты.
- Биографическая информация, которая не соответствует личности заявителя.
- Неспособность своевременно выполнять задания или отвечать на задания.
- Невозможность своевременно связаться с ними, особенно с помощью способов мгновенного обмена сообщениями.
- Обращение к коллегам с просьбой использовать их личную информацию для получения других контрактов.

*Схема деятельности специалистов в сфере ИТ из КНДР*




## ПОТЕНЦИАЛЬНЫЕ МЕРЫ СНИЖЕНИЯ РИСКА

*Для компаний, предлагающих платформы для фрилансеров и платежные платформы*

- Проверяйте документы, представленные в рамках рассмотрения предложений и процедур комплексной проверки контрактов, например, самостоятельно проверяйте выставленные счета и договоры на выполнение работ, связываясь с указанными клиентами с использованием контактной информации, указанной в базах данных для бизнеса, а не контактной информации, указанной в представленной документации.

- Внимательно изучайте представленные удостоверения личности на предмет подделки, при необходимости обращайтесь за помощью в местные правоохранительные органы. Отклоняйте изображения низкого качества, предоставленные для подтверждения личности.

- Проверьте существование любых веб-сайтов, указанных при создании учетных записей; дополнительно проверяйте учетные записи, при регистрации которых использовались прекратившие деятельности веб-сайты.

- В рамках процессов проведения первоначальной комплексной проверки при заключении контрактов и обновления правил требуйте предоставления видеозаписи, подтверждающей личность, или проводите видеоинтервью для подтверждения личности.

- Регулярно используйте возможности проверки портов, чтобы определить, осуществляется ли удаленный доступ к платформе через программное обеспечение для совместного использования рабочего стола, VPN или VPS, особенно если использование такого программного обеспечения или VPN для доступа к учетным записям не является стандартной практикой.

- Автоматически инициируйте дополнительную проверку в отношении учетных записей клиентов и разработчиков, использовавших одну и ту же или похожую документацию при создании учетных записей или одни и те же учетные записи цифровых платежных сервисов.

- Автоматически инициируйте дополнительную проверку в случае использования одинаковых или похожих шаблонов документов для тендеров и проектных коммуникаций в разных учетных записях разработчиков.

- Автоматически инициируйте дополнительную проверку в отношении нескольких учетных записей разработчиков, получивших высокие оценки от одного клиента за короткий период, особенно если для создания учетных записей использовалась схожая или идентичная документация.

- Автоматически инициируйте дополнительную проверку в отношении учетных записей разработчиков с высокими ставками, а также учетных записей с низким количеством принятых проектных предложений по сравнению с количеством размещенных заявок. Кроме того, уделяйте особое внимание учетным записям с большим числом заявок на участие в проектах по сравнению с числом входов в учетную запись.

- Не допускайте никакой активности в новых учетных записях до полного прохождения проверки.

- Обеспечьте дополнительную проверку в отношении недавно созданных учетных записей.

***Для компаний, осуществляющих наем программистов и разработчиков на фриланс-платформах***

- Проводите видеоинтервью для проверки личности потенциального внештатного работника.

- Проводите проверку биографических данных перед приемом на работу, тест на наркотики и используйте вход в систему с помощью отпечатков пальцев/биометрических

данных для подтверждения личности и заявленного местонахождения. Избегайте платежей в виртуальной валюте и требуйте, чтобы данные в банковских реквизитах соответствовали данным в других идентифицирующих документах.

- Будьте особенно осторожны, взаимодействуя с внештатными разработчиками через приложения для удаленного сотрудничества, такие как приложения для удаленного рабочего стола. Рассмотрите возможность отключения приложений для удаленного сотрудничества на любом компьютере, предоставленном внештатному разработчику.

- Проверьте сведения об образовании и опыте работы непосредственно в перечисленных компаниях и учебных заведениях, используя контактную информацию, полученную через поисковую систему или другую базу данных для бизнеса, а не непосредственно от потенциального сотрудника или из его профиля.

- Убедитесь в отсутствии расхождений в написании имени, сведениях о гражданстве, месте работы, контактной информации, сведениях об образовании, опыте работы и других данных в профилях разработчиков на фриланс-платформах, профилях в социальных сетях, на внешних сайтах-портфолио, в профилях платежных платформ, а также несоответствий оценочному местоположению и часовому поясу. Будьте особенно внимательны в отношении простых сайтов-портфолио, профилей в социальных сетях или профилей разработчиков;

- С осторожностью относитесь к просьбам разработчика общаться на отдельной платформе за пределами фриланс-платформы, на которой компания изначально нашла ИТ-специалиста.

- При отправке разработчику документов или необходимого для работы оборудования, например, ноутбука, осуществляйте отправку только по адресу, указанному в документах, удостоверяющих личность разработчика, а если разработчик просит отправить ноутбук или другие предметы по другому адресу, запросите дополнительные документы. Проявите настороженность, если разработчик не может получать отправления по адресу, указанному в его идентификационных документах.

- Будьте бдительны в отношении несанкционированных мелких транзакций, которые могут мошеннически проводиться ИТ-подрядчиками. Есть случай, когда ИТ-специалисты из КНДР, работавшие разработчиками в американской компании, обманным путем снимали деньги с платежного счета американской компании и украли более 50 000 долларов США, осуществив 30 транзакций на небольшие суммы в течение нескольких месяцев. Американская компания не знала ни о том, что разработчики были из Северной Кореи, ни о постоянных хищениях, поскольку суммы были незначительными.

## ПОСЛЕДСТВИЯ УЧАСТИЯ В ЗАПРЕЩЕННОЙ ИЛИ ПОДПАДАЮЩЕЙ ПОД САНКЦИИ ДЕЯТЕЛЬНОСТИ

Физические и юридические лица, поддерживающие деятельность, связанную с ИТ-специалистами из КНДР, или вовлеченные в нее, включая обработку соответствующих финансовых транзакций, должны знать о возможных юридических последствиях участия в запрещенной или подпадающей под санкции деятельности.

В резолюциях Совета Безопасности ООН 2321, 2371 и 2397 подчеркивается, что получаемые от работающих за рубежом специалистов из КНДР доходы способствуют реализации программ КНДР по созданию ядерного оружия и баллистических ракет. Резолюция 2375 Совета Безопасности ООН запрещает государствам-членам ООН выдавать новые разрешения на работу или продлевать истекшие разрешения гражданам КНДР, находящимся под их юрисдикцией, в связи с въездом на их территорию, если это заранее не одобрено Комитетом 1718 Совета Безопасности ООН. Резолюция 2397 Совета Безопасности ООН требует от всех государств-членов репатриировать до 22 декабря 2019 года граждан КНДР, получающих доход в их юрисдикции, независимо от того, были ли выданы разрешения на работу для данных граждан КНДР и когда они были выданы.

Управление по контролю за иностранными активами Министерства финансов США (OFAC) имеет право налагать финансовые санкции на любое лицо, в отношении которого установлено, что оно, среди прочего:

- занимается значительной деятельностью от имени правительства КНДР или Трудовой партии Кореи, которая подрывает кибербезопасность;
- осуществляет деятельность от имени КНДР в ИТ-отрасли;
- вовлечено в иные вредоносные действия с использованием компьютерных технологий;
- участвовало минимум в одном эпизоде крупного экспорта из КНДР или импорта в КНДР любых товаров, услуг или технологий;
- осуществляло продажу, поставку, передачу или покупку, прямо или косвенно в/из КНДР или любому лицу/от любого лица, действующего от имени или по поручению правительства КНДР или Трудовой партии Кореи, программного обеспечения, в результате чего любой доход или полученные товары могли принести пользу правительству КНДР или Трудовой партии Кореи; или
- оказывало в значительном размере помощь, спонсорство или предоставляло финансовую или материально-техническую поддержку, товары или услуги с целью содействия правительству КНДР или Трудовой партии Кореи.

Например, в 2018 году Соединенные Штаты включили в санкционный список китайскую технологическую компанию Yanbian Silverstar Network Technology Co. Номинально эта компания была китайской ИТ-компанией, но в действительности она находилась под управлением и контролем представителей Северной Кореи. Эта компания также создала российскую подставную фирму Volasys Silver Star, чтобы обойти требования идентификации на форумах по поиску работы для фрилансеров.

Кроме того, если министр финансов США по согласованию с государственным секретарем определит, что иностранное финансовое учреждение сознательно вело или содействовало торговле с КНДР в значительном размере или сознательно заключило или содействовало заключению крупной сделки от имени лица, указанного в Исполнительном распоряжении по КНДР или в Исполнительном распоряжении 13382 (по распространителям оружия массового поражения и их сторонникам) по деятельности, связанной с КНДР, то такое учреждение может, помимо других возможных ограничений, потерять возможность иметь корреспондентский или сквозной счет в США.

OFAC расследует очевидные нарушения своих положений о санкциях и осуществляет правоприменительные полномочия, как указано в Руководстве по применению экономических санкций, опубликованных в Своде федеральных нормативных актов 31, часть 501, приложение A. Лица, нарушившие Положение о санкциях в отношении Северной Кореи, опубликованных в Своде федеральных нормативных актов 31, часть 510, могут быть подвергнуты денежным штрафам за гражданское правонарушение в размере до максимального штрафа, предусмотренного законодательством, или двойной стоимости соответствующей сделки в зависимости от того, что будет больше.

Кроме того, Закон о противодействии противникам Америки посредством санкций (CAATSA; Публичный закон 115-44), раздел 321(b) (Кодекс законов США 22, § 9241a), который внес поправки в Закон о санкциях и усилении политики в отношении Северной Кореи от 2016 года (Кодекс законов США 22, § 9241 и далее. ), создал опровержимую презумпцию того, что значимые товары, изделия, продукция и предметы, добытые, произведенные или изготовленные полностью или частично выходцами из Северной Кореи или ее гражданами в любой точке мира, являются товарами, произведенными с применением принудительного труда, и поэтому запрещенными к импорту в соответствии с Законом о тарифах 1930 года (Кодекс законов США 19, § 1307). Это означает, что данные товары не подлежат ввозу в любой порт США и могут быть подвергнуты задержанию, аресту и конфискации. Нарушения могут привести к административным штрафам, а также к уголовному преследованию. Однако в соответствии с CAATSA такие товары могут быть импортированы в США, если комиссар Бюро таможенного и пограничного контроля (БТПК) найдет ясные и убедительные доказательства того, что товары не были произведены с использованием труда осужденных, принудительного труда или кабального труда. Запрет на импорт товаров, произведенных с использованием труда осужденных, принудительного или кабального труда в рамках уголовного наказания (включая

принудительный или кабальный детский труд), был введен в соответствии с Законом о тарифах 1930 года и в таком виде действует уже почти 90 лет.

Министерство юстиции отвечает за проведение расследований и судебное преследование в соответствии с применимыми федеральными законами, включая Закон о международных чрезвычайных экономических полномочиях (IEEPA), Кодекс законов США 50, § 1701 и последующие, Закон о банковской тайне (BSA) и Кодекс законов США 31, §§ 5318 и 5322. Согласно IEEPA преступлением является умышленное нарушение, попытка нарушения, сговор с целью нарушения или побуждение к нарушению любой лицензии, приказа, постановления или запрета, изданного в соответствии с IEEPA, включая любое связанное с КНДР исполнительное распоряжение (например, Исполнительные распоряжения 13722 и 13810), Исполнительное распоряжение 13382, а также Положение о санкциях в отношении Северной Кореи, опубликованное в Своде федеральных нормативных актов 31, часть 510. Лицам, умышленно нарушившим IEEPA, грозит до 20 лет лишения свободы, штрафы в размере до 1 миллиона долларов США или в двукратном размере полученного дохода, в зависимости от того, что будет больше, а также потенциальная конфискация всех средств, задействованных в таких сделках. Закон о банковской тайне требует, чтобы финансовые учреждения, помимо прочего, внедряли эффективные программы противодействия отмыванию доходов, полученных преступным путем, а также подавали определенные отчеты в Управление Министерства финансов США по борьбе с финансовыми преступлениями. Лицам, нарушившим BSA, может грозить лишение свободы на срок до 5 лет, штраф в размере до 250 000 долларов США и возможная конфискация имущества, использовавшегося при совершении таких нарушений. Корпорации и другие организации, нарушающие IEEPA, BSA и другие применимые федеральные законы, также могут подвергаться уголовному преследованию. Министерство юстиции также сотрудничает с зарубежными партнерами для обмена доказательствами при проведении расследований по уголовным делам и судебных преследований в США и за рубежом.

На основании Свода федеральных нормативных актов 31, § 5318(k), министр финансов или генеральный прокурор могут вызвать в суд иностранное финансовое учреждение, имеющее корреспондентский банковский счет в США, для получения документов, хранящихся за рубежом. Если секретарь Казначейства или генеральный прокурор направит письменное уведомление финансовому учреждению США о том, что иностранное финансовое учреждение проигнорировало данное требование, такое финансовое учреждение США должно прекратить корреспондентские банковские отношения в течение десяти рабочих дней. В противном случае на финансовое учреждение США могут ежедневно налагаться административные штрафы.

## *ВОЗНАГРАЖДЕНИЕ ЗА ПОМОЩЬ ПРАВОСУДИЮ*

Если у вас есть информация о незаконной деятельности КНДР в киберпространстве, включая прошлые или текущие операции, то, предоставив такую информацию через программу «Вознаграждение за помощь правосудию» Государственного департамента, вы можете получить

награду в размере до 5 миллионов долларов США. Дополнительную информацию можно найти по ссылке https://rewardsforjustice.net/index/?north-korea=north-korea.

## ПРИЛОЖЕНИЕ

### *Отчеты экспертной группы ООН об ИТ-специалистах из КНДР*

Поддержку Комитету по санкциям Совета Безопасности ООН 1718 в отношении КНДР оказывает Группа экспертов (далее — «Группа»), которая собирает, изучает и анализирует информацию от государств-членов ООН, соответствующих органов ООН и других сторон о выполнении мер, изложенных в резолюциях Совета Безопасности ООН в отношении КНДР. Группа также дает рекомендации о том, как улучшить выполнение санкций, предоставляя Комитету 1718 промежуточный и окончательный отчеты. Эти отчеты можно найти по ссылке https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports

Группа расследовала многочисленные случаи в отношении ИТ-специалистов из КНДР, например, подчиненных Департамента военной промышленности (ДВП), созданного ООН, и предоставила информацию об этих расследованиях в полугодовых отчетах Группы, включая следующие:

Впервые Группа сообщила об ИТ-специалистах из КНДР в своем среднесрочном отчете за 2019 год, отметив, что ДВП, который играет ведущую роль в развитии ядерной программы и программы баллистических ракет КНДР, использует подчиненные ему торговые корпорации для размещения за рубежом ИТ-специалистов из КНДР, таких как программисты и разработчики программного обеспечения, чтобы зарабатывать иностранную валюту. На момент подготовки отчета ИТ-специалисты из КНДР, находящиеся в Европе, Азии, Африке и на Ближнем Востоке, использовали зарубежные веб-сайты для получения работы в качестве фрилансеров, скрывая свою личность. Наряду с выполнением работ в сфере информационных технологий, не являющихся вредоносными, ИТ-специалисты из КНДР осуществляли незаконную деятельность, связанную с кражей активов, таких как виртуальные валюты, для помощи киберпреступникам из КНДР в обходе финансовых санкций.

Группа продолжила расследование в отношении ИТ-специалистов из КНДР в своем Заключительном отчете за 2020 год и пришла к выводу, что большинство зарубежных ИТ-специалистов из КНДР работают в компаниях, подчиняющихся ДВП. К 2019 году ДВП подозревал в том, что он направил за границу не менее 1000 ИТ-специалистов с целью получения дохода, часто используя подчиненные организации или подставные компании. Однако из-за используемых способов маскировки истинное число ИТ-специалистов за рубежом и в КНДР было неясно. Группа отметила, что ИТ-специалисты из КНДР используют несколько способов для получения работы в сфере ИТ в качестве фрилансеров без раскрытия своей личности, в том числе создавая учетные записи на платформах для разработчиков-фрилансеров и работая с ни о чем не подозревающими клиентами по всему миру, особенно из Китая, России, Украины, Сербии, Канады и США. Группа подробно расследовала несколько конкретных случаев, которые произошли с командами ИТ-специалистов из КНДР и связанными с ними компаниями в Китае, Непале и Вьетнаме.

Группа провела расследование в отношении нескольких команд ИТ-специалистов из КНДР, базирующихся в Китае и России, подробно описав результаты расследования в своем среднесрочном отчете за 2020 год. Группа отметила, что сотни ИТ-специалистов из КНДР, подконтрольных ДВП, работали в Китае в 2019 и 2020 годах, незаконно получая доступ к учетным записям на фриланс-платформах, используя имена граждан третьих стран. Далее Группа отметила, что в 2019 и 2020 годах в России действовали многочисленные команды подконтрольных ДВП ИТ-специалистов из КНДР, которые использовали поддельные иностранные документы для доступа к фриланс-платформам в сфере информационных технологий, сайтам виртуальных валют и платежным сайтам.

Согласно заключительному отчету Группы за 2021 год ИТ-специалисты из КНДР могут обойти усилия работодателей по проявлению должной осмотрительности и протоколы идентификации клиентов/противодействия отмыванию доходов, полученных преступным путем, используя способы маскировки, аналогичные тем, которые используются КНДР для доступа к международной финансовой системе, включая предоставление ложных идентификационных данных, использование VPN-сервисов и создание подставных компаний. Группа далее отметила, что большинство связанных с КНДР учетных записей действуют из мест расположения в Китае. Чтобы избежать проверки, после установления контакта с потенциальными клиентами, желающими получить услуги в сфере ИТ, владельцы этих учетных записей переходят на общение за пределами площадки. Связанные с КНДР пользователи также нацелены на платформы для ИТ-фрилансеров с низким уровнем безопасности или менее строгими процедурами проверки благонадежности. Группа особо отметила опасности, с которыми сталкиваются платформы для ИТ-фрилансеров в связи с выполнением обязательств по соблюдению санкций и непреднамеренным облегчением доступа КНДР к международным платежным системам, рекомендовав государствам-членам ООН работать с внештатными ИТ-компаниями для продвижения и укрепления потенциала и возможностей по соблюдению санкций.