НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

О рекомендациях по использованию средств удалённого доступа

ALRT-20240205.1 | 5 февраля 2024 г.

TLP: WHITE

Описание	В условиях проведения компьютерных атак на российские информационные ресурсы НКЦКИ просит принять к сведению предыдущие рекомендации (ALRT-20220302.1, ALRT-20220329.1 и ALRT-20200320) об использовании внешних сервисов для организации удаленного доступа к информационной инфраструктуре организации. Удаленный доступ несет в себе риск компрометации компонентов информационной инфраструктуры. Это подтверждается недавним фактом проведения компьютерной атаки на ресурсы компании AnyDesk, выпускающей решения для удаленного доступа. В результате злоумышленники получили доступ к производственным системам компании. В связи с этим просим придерживаться следующих рекомендаций:
Рекомендации	1. По возможности ограничьте удаленный доступ извне ко всем сервисам и устройствам в ИТС, кроме безусловно необходимых. 2. Обратите особое внимание на учетные записи, применяемые для удаленного подключения как своих работников, так и специалистов подрядных организаций, в том числе выполняющих задачи по технической поддержке. 3. Убедитесь, что средства антивирусной защиты и межсетевого экранирования надлежащим образом настроены и функционируют на всех узлах ИТС. 4. Проверьте обновление всех сервисов и оборудования, которые используются для удаленного доступа (VPN, устройства сетевой инфраструктуры). 5. Используйте удаленный доступ в сеть организации строго с двухфакторной авторизацией. 6. Запретите использовать сторонние средства удаленного доступа в корпоративную сеть, которые подключаются через промежуточные сервера и самостоятельно проводят авторизацию и аутентификацию.