2023 АНБ Кибербезопасность

Год в обзоре.

2 0 2 3 АНБ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

{Год в обзоре

Добро пожаловать

Со времен Второй мировой войны Агентство национальной безопасности (АНБ) и его предшественники защищали наиболее конфиденциальную информацию Соединенных Штатов. Поскольку технологические достижения создали более взаимосвязанный мир с постоянно растущими угрозами, миссия АНБ расширилась. АНБ взяло на себя новые обязанности и оперативные полномочия, чтобы обеспечить безопасность наших сетей.

Сегодня миссия АНБ по кибербезопасности объединяет знания в области криптографии, разведку иностранных сигналов, анализ уязвимостей, оборонительные операции и многое другое для предотвращения и искоренения киберугроз в трех ключевых областях.

Кибербезопасность АНБ защищает и защищает:

- Системы национальной безопасности (СНБ):Сети, которые содержат секретную информацию или иным образом имеют решающее значение для военной и разведывательной деятельности США. Крайне важно, чтобы эти сети оставались безопасными, чтобы обеспечить готовность боевых возможностей США к выполнению миссий и защитить наиболее конфиденциальную информацию страны.
- Министерство обороны (DoD):Военные службы и боевые командования США, а также правительственные учреждения и ведомства США, связанные с национальной безопасностью.
- Оборонно-промышленная база (ОПБ):Постоянно растущая группа компаний, которые проектируют, разрабатывают, эксплуатируют и обслуживают критически важные системы, платформы и технологии Министерства обороны, необходимые для защиты нации. Их продукты, услуги и возможности жизненно важны для безопасности США и наших союзников.

Стремясь быть более прозрачным, АНБ публикует ежегодный обзор, в котором делится информацией об усилиях по обеспечению кибербезопасности, которые лучше обеспечивают защиту США от высокоприоритетных киберугроз. Усилия АНБ по обеспечению безопасности наиболее чувствительных систем странытакже помогите вашей кибербезопасностипотому что АНБ каскадирует эти решения через общественное руководство и взаимодействует с ключевыми поставщиками технологий, чтобы помочь им повысить безопасность своих продуктов и услуг.

> ПосещатьАНБ.gov/cybersecurity получить доступ к отчету в цифровом виде. Оставьте отзыв АНБ по кибербезопасности или задайте вопросы по электронной почте.cybersecurity@nsa.gov

Верхнее и нижнее изображения предоставлены Getty Images, среднее фото предоставлено Министерством обороны США.

СОДЕРЖАНИЕ

Письмо

От директора АНБ

В моей роли директора Агентства национальной безопасности (АНБ) мне выпала честь возглавить рабочую группу, которая поддерживает каждый компонент разведывательного сообщества и Министерства обороны посредством его миссий по радиоразведке и кибербезопасности.

АНБ является мировым лидером в создание и взлом кодов. Талантливые люди в нашем Агентстве неустанно работают, чтобы защитить нашу страну от иностранных противников.

Вклад АНБ имеет решающее значение в нынешнюю эпоху стратегическая конкуренция, в котором мировые державы конкурируют в экономическом, военном, технологическом и дипломатическом отношении.

Китайская Народная Республика (КНР) стала основным вызовом Соединенным Штатам и как конкурент, имеющий как намерение, так и способность изменить международный порядок в соответствии со своими собственными замыслами. КНР, противник, уникальный по размаху, масштабу и сложности угроз, которые она представляет, заявила о своем желании стать одной из ведущих мировых держав.

Россия остается серьезной угрозой и продолжает угрожать региональной безопасности и глобальной стабильности из-за своего игнорирования международных норм и своей готовности использовать свое оружие для нападения на гражданское население и критически важную инфраструктуру. Мы стали свидетелями показательного примера этого во время незаконного вторжения России в Украину. Россия также развернула информационные операции, направленные на ослабление демократических институтов по всему миру.

Нам необходимо быть в состоянии реагировать на угрозы со стороны КНР, России и других глобальных противников сегодня и в будущем. Мы должны оставаться впереди наших глобальных конкурентов которые постоянно стремятся изменить глобальную информационную среду и мировой порядок, каким мы его знаем.

Такие органы власти, как раздел 702 Закона о надзоре за внешней разведкой (FISA), позволяют нам это делать. Раздел 702 FISA — это ключевой орган внешней разведки, который помогает обеспечивать безопасность Соединенных Штатов и их союзников. Разведывательные данные из раздела 702 используются каждый день, чтобы защитить нацию от критических угроз, информировать правительство США о стратегии и спасти жизни американцев. Поскольку любое упущение в этом законе будет иметь ослепляющий эффект на наше понимание враждебных иностранных субъектов, действующих за пределами наших границ, мы ожидаем, что Конгресс повторно санкционирует раздел 702.

Полномочия, которыми доверено АНБ, позволяют АНБ решать самые важные проблемы национальной безопасности, в том числе информационная безопасность. В последнее время мы стали свидетелями изменения характера конфликтов: Киберпространство — это оспариваемое пространство. Стало ясно, что переход от конкуренции к кризису и конфликту теперь может произойти за недели, дни или даже минуты. Каждый день в АНБ мы стремимся предотвращать и искоренять киберугрозы системам национальной безопасности США, Министерству обороны и Оборонно-промышленной базе (DIB).

Новая Национальная стратегия кибербезопасности четко и целенаправленно ориентирована на использование международного партнерства для достижения общих целей в области защиты программного обеспечения, критически важной инфраструктуры и глобальных сетей, демонтажа и борьбы с участниками программ-вымогателей, расширения оперативного сотрудничества в киберпространстве и создания возможностей обнаружения инцидентов и реагирования на них. .

Наши отношения в области разведки и кибербезопасности с нашими союзниками и партнерами являются стратегическим активом, который будет все больше влиять на нашу конкуренцию с нашими соперниками, особенно в технологической конкуренции.

Глобальный ландшафт становится все более сложным, поскольку технологии, которые мы используем в киберпространстве, продолжают развиваться. Одним из таких примеров являетсяИскусственный интеллект (ИИ), который способен перевернуть с ног на голову несколько секторов общества одновременно. Мы должны опережать наших глобальных конкурентов в гонке, чтобы понять и использовать его потенциал, а также защитить себя от враждебного использования. В АНБ мы располагаем уникальными возможностями для этого, объединяя наш глубокий технический опыт, понимание угроз и полномочия для поддержки этих усилий.

Недавно я объявил, что АНБ объединяет свою различную деятельность, связанную с безопасностью искусственного интеллекта, в новое подразделение — Центр безопасности искусственного интеллекта АНБ. Центр безопасности искусственного интеллекта, расположенный в нашем Центре сотрудничества в области кибербезопасности, позволит нам тесно сотрудничать с разведывательным сообществом, Министерством обороны, промышленной базой, национальными лабораториями, научными кругами, а также выбирать иностранных партнеров для сотрудничества.обеспечить устойчивое преимущество США в области искусственного интеллекта.

Принципы и ценности АНБ, а также нашикультура соблюдения и защиты частной жизни и гражданских свобод, послужили основой для успехов в области кибербезопасности, подробно описанных в этом отчете, и будут продолжать служить основой АНБ в будущем.

В АНБ наши люди и наше партнерство имеют решающее значение. Сотрудники АНБ твердо верят в важность доверия, оказанного им клятвой, которую они поклялись соблюдать. Наше глубокое и долгосрочное партнерство позволяет намвместе преодолевать угрозы и масштабировать решения, чтобы сделать эту страну – и наших союзников - более безопасный.От имени АНБ я выражаю искреннюю благодарность за работу, которую выполняют все наши партнеры в этой сфере, поскольку наша коллективная киберустойчивость и оперативное реагирование на угрозы становятся лучше, когда мы работаем вместе.

ПОЛ М. НАКАСОНЕ

Генерал армии США

командующий Киберкомандованием США,

Директор Агентства национальной безопасности/начальник Центральной службы безопасности

Письмо

От директора по кибербезопасности АНБ

Управление кибербезопасности АНБ было создано с целью установления связей с промышленностью и другими партнерами. Эта тенденция сохранилась и в прошлом году, поскольку мы больше, чем когда-либо прежде, стали использовать партнерские отношения. Мы концентрируемся на том, чтобы взять то, что знаем, и превратить это в действия, которые защищать сети и наносить ущерб нашим противникам новыми способами. Наше внутреннее и международное партнерство помогает нам вместе противодействовать угрозам,масштабировать решения кибербезопасностии оказать еще большее влияние.

Когда мы что-то знаем, это имеет ценность только тогда, когда защитники сети могут предпринять с этим реальные действия. К двунаправленный обмен информацией в несекретной среде вместе с нашими партнерами мы улучшаем как кибербезопасность, так и национальную безопасность.

The объединенный талант наших партнеровЭто величайшее конкурентное преимущество, которое мы имеем, чтобы противостоять все более изощренным угрозам, которые мы наблюдаем сегодня.

За последний год мы выявили множество угроз кибербезопасности. Работая с отраслевыми и международными партнерами, мы определили индикаторы компрометации, связанные с Спонсируемый государством киберпреступник Китайской Народной Республики (КНР) использует методы выживания за счет земли – используя встроенные сетевые инструменты для обхода защиты, не оставляя следов – для нападения на сети в критической инфраструктуре США. .Мы воспользовались услугами нескольких организаций частного сектора, чтобы лучше понять эту угрозу, и выпустили руководство, которое поможет сетевым защитникам выслеживать и обнаруживать этот тип вредоносной активности в своих системах и критически важных сетях.

Работа с партнерскими агентствами также позволила намвыявил сложную российскую вредоносную программу Snake для кибершпионажа, которая используется более чем в 50 странах мира. Вместе мы приписали операцию «Змея» известному подразделению Центра 16 Федеральной службы безопасности России. Технические подробности, которые мы опубликовали вместе с партнерами, позволили Федеральному бюро расследований (ФБР) работать и помогли многим организациям найти и отключить вредоносное ПО по всему миру.

Кроме того, сотрудничество с отраслевыми партнерами привело к обнаружению уязвимости в серверах Citrix, которая могла привести к краже информации с оборонно-промышленной базы. Благодаря этому партнерству,уязвимость нулевого дня была выявлена и исправлена, а количество уязвимых серверов по стране значительно сократилось .

Наш Центр сотрудничества в области кибербезопасности (ССС) позволяет нам создавать коалиции для совместного обмена информацией и устранения подобных угроз. В этом году ССС утроил свое партнерство, поэтому теперь мы сотрудничаем более чем в750 открытых и крепких отношенийв промышленности и правительстве, что позволяет нам масштабировать методы предотвращения, обнаружения и смягчения последствий для миллиарды конечных точек по всему миру. КТС масштабировала свою программу кибербезопасности как программу услуг, включив малый и средний бизнес в цепочку поставок оборонно-промышленной базы (DIB). Эти годы400% увеличение количества обращений к нашим услугампомогает гарантировать, что нашим критически важным партнерам в сфере обороны, включая малый и средний бизнес, не придется защищать свои системы в одиночку. Наши партнерские отношения позволяют нам двигаться вперед и активно делиться идеями, делая то, что нам поручено: помогать защищать оборону нашей страны, ее наиболее важные сети и DIB.

Одной из новых угроз (и возможностей) является искусственный интеллект (ИИ). Технологии искусственного интеллекта и машинного обучения развиваются и распространяются быстрее, чем компании и правительства могут формировать нормы, создавать стандарты и обеспечивать положительные результаты. Хотя эти инструменты могут обеспечить новые удивительные защитные возможности, они также могут расширить возможности злоумышленников. Недавно созданное АНБЦентр безопасности искусственного интеллектав нашем Центре сотрудничества в области кибербезопасности является новым координатором Агентства, который применяет уникальные знания, полученные в результате анализа сигналов и технологий АНБ, а также сотрудничает с промышленностью, чтобы помочь коллегам из отрасли понимать, предотвращать и смягчать угрозы в экосистеме искусственного интеллекта. Центр будет служить координатором для разработки передового опыта, методологии оценки и систем управления рисками, в то время как мы стремимся способствовать безопасному внедрению возможностей искусственного интеллекта.

Мы также добились прогресса в марафоне по переходу на квантовостойкая криптографиядля защиты наших сетей, технологий, на которые мы полагаемся, и наших оружейных платформ. Мы подготовили криптографические дорожные карты для каждого партнера боевого командования США по коалиции, чтобы помочь нашим партнерам определить, куда им необходимо инвестировать, чтобы защититься от современных киберугроз и стать полностью совместимыми с силами США и их союзников.

В конечном итоге, эти важные результаты достигаются благодаря людям из АНБ и наших партнерских организаций, которые внедряют инновации, выдвигают блестящие идеи и оперативно реализуют их, чтобы обезопасить нашу страну и наших партнеров сейчас и в будущем.

С уважением,

Роб Джойс
Директор АНБ по кибербезопасности

“

Вместе сообщество кибербезопасности становится намного лучше благодаря силе партнерства.

{ Роб Джойс
Директор АНБ по кибербезопасности

Бдительность

К национальным угрозам и приоритетам

Противодействие глобальным угрозам

Вместе с американскими и международными партнерами АНБ продолжает расширять свое влияние в борьбе с растущими глобальными угрозами и изощренными противниками.

В то время как правительство США полагается на уникальные данные внешней радиоразведки АНБ для принятия ключевых решений, сотрудничество государственного и частного секторов строится на этой основе, чтобы лучше понять угрозы и способы противодействия им.

Каждая организация привносит свои уникальные возможности, полномочия и знания, чтобы нарисовать более широкую картину, тем самым повышая способность АНБ предотвращать и искоренять некоторые из наиболее серьезных киберугроз в мире.

Выявление и смягчение вредоносной деятельности Китайской Народной Республики

Совместно с ключевыми отраслевыми партнерами АНБ выявило спонсируемого государством киберпреступника Китайской Народной Республики (КНР), который использовал встроенные сетевые инструменты для нападения на критически важную инфраструктуру США. Чтобы помочь сетевым защитникам отслеживать и обнаруживать этот тип вредоносной активности КНР в своих системах, АНБ координировало действия с американскими и международными партнерами, чтобы публично опубликовать«Спонсируемый государством кибер-актер Китайской Народной Республики живет за счет земли, чтобы избежать обнаружения» совместные консультации по кибербезопасности. В рекомендациях представлен обзор рекомендаций по поиску и связанных с ними передовых практик, а также примеры команд субъекта и сигнатур обнаружения.

> Кибератеры считают, что проще и эффективнее использовать возможности, уже встроенные в критически важные инфраструктурные среды. Спонсируемый государством субъект живет за счет земли, используя встроенные сетевые инструменты, чтобы обойти нашу защиту и не оставлять после себя никаких следов, поэтому нам крайне важно работать вместе, чтобы найти и удалить субъекта из наших критически важных сетей.
>
> Роб Джойс
> Директор АНБ по кибербезопасности

В другом случае, когда отраслевой партнер обнаружил субъектов КНР, нацеленных на критически важные организации DIB, используя уязвимость нулевого дня, АНБ немедленно поделилось техническими индикаторами с партнерами DIB, чтобы обеспечить обнаружение в их сетях. Уязвимость была специально нацелена на широко используемые устройства в DIB, поэтому ежедневное взаимодействие АНБ с отраслью в течение двухмесячного периода помоглосорвать и смягчить кампанию.

Охота на «змеиное» вредоносное ПО российской разведки

По согласованию с партнерами,АНБ выявило сложную российскую вредоносную программу Snake для кибершпионажа, которая используется более чем в 50 странах мира. АНБ, Национальные силы кибербезопасности USCYBERCOM, ФБР, Агентство кибербезопасности и безопасности инфраструктуры, Канадский центр кибербезопасности, Австралийский центр кибербезопасности, Бюро безопасности правительственных коммуникаций Новой Зеландии и Национальный центр кибербезопасности Великобритании приписали операции Snake известное подразделение Центра 16 Федеральной службы безопасности России. Эта инфраструктура была обнаружена в Северной Америке, Южной Америке, Европе, Африке, Азии и Австралии, включая США и даже Россию. Технические подробности, опубликованные совместно с партнерами, помогли ФБР, сотрудничающему со многими организациями, обнаружить и отключить вредоносное ПО по всему миру.

Международное сотрудничество для выпуска руководства

Сотрудничая с правительством США и международными партнерами, АНБ позволило расширить обмен информацией посредством рекомендаций по кибербезопасности относительно угроз национальным государствам.

Впервые мы сотрудничали с Национальным полицейским агентством Японии и Японским центром готовности к инцидентам и стратегии кибербезопасности, АНБ вместе с ФБР и Агентством кибербезопасности и безопасности инфраструктуры США (CISA), выпустили совместные рекомендации по кибербезопасности, в которых подробно описывается деятельностьСвязанные с КНР киберпреступники, известные как BlackTech. BlackTech продемонстрировала возможности модификации прошивки маршрутизатора без обнаружения и использования отношений доверия домена маршрутизаторов для перехода от международных дочерних компаний к их материнским компаниям в Японии и США.

Еще одним первым событием стало то, что АНБ работало с Национальной разведывательной службой Республики Корея, Национальным полицейским управлением и Министерством иностранных дел, а также с нашими партнерами из ФБР и Госдепартамента США, чтобы совместно выпустить рекомендацию по кибербезопасности, в которой подчеркивается использованиесоциальная инженерия кибер-актеров, спонсируемых государством Корейской Народно-Демократической Республики обеспечить глобальную эксплуатацию компьютерных сетей против лиц, работающих в исследовательских центрах и аналитических центрах, академических учреждениях и средствах массовой информации.

Министерство обороны (DoD) выполняет функции Агентства по управлению отраслевыми рисками для оборонно-промышленной базы (DIB). В этой роли министерство взаимодействует с компаниями DIB, отслеживает и определяет приоритетность угроз, контролирует управление инцидентами и предоставляет техническую помощь, среди прочего. обязанности. Инициативы Департамента по кибербезопасности DIB включают Программу кибербезопасности DIB, Среду совместного обмена информацией DoD-DIB Центра киберпреступности Министерства обороны США,**Центр сотрудничества в области кибербезопасности Агентства национальной безопасности и система устойчивой безопасности.**

Выдержка из сводки киберстратегии Министерства обороны США
выпущен в сентябре 2023 г.

Партнерство

С промышленностью и защитой оборонно-промышленной базы

Защита оборонно-промышленной базы (DIB)

Хотя у многих людей DIB ассоциируется с крупными оборонными подрядчиками, более 70% DIB составляют малые предприятия. После подписания контракта с Министерством обороны эти компании часто становятся мишенью для государственных субъектов. Малый бизнес, как правило, не имеет ресурсов для защиты только от действий национального государства. АНБ работает с большими и малыми компаниями DIB — важными партнерами АНБ в обороне.
- привлечение ведущего в мире агентства по созданию и взлому кодов на их стороне.

> Мы находимся в авангарде перемен, чтобы поделиться своими идеями с частным сектором. Мы видим силу опыта АНБ так, как никогда раньше.
>
> Морган Адамски
> Руководитель Центра сотрудничества в области кибербезопасности

АНБ предоставляет бесплатные услуги по кибербезопасности подрядчикам Министерства обороны США, основанный на многолетнем опыте АНБ в создании и взломе кодов. Эти услуги предназначены для защиты от атак АНБ на иностранных противников, нацеленных на DIB, и основаны на уникальных знаниях и аналитике АНБ. В 2023 году, благодаря активным усилиям по распространению информации и развитию, АНБ увеличило набор служб кибербезопасности почти на 400%. В настоящее время АНБ оказывает помощь в области кибербезопасности более чем 600 компаниям в цепочке поставок Министерства обороны, включая поставщиков, у которых может не хватать собственных ресурсов в области кибербезопасности.

Хотя эти услуги открыты для любой компании с действующим генеральным контрактом или субподрядом Министерства обороны, в 2023 году АНБ запустило несколько новых кампаний, чтобы уделить приоритетное внимание компаниям, поддерживающим:

1. Зона ответственности Индо-Тихоокеанского командования США
2. Российско-украинский конфликт и
3. Приоритетные системы вооружения Министерства обороны

Какая отрасль АНБ Партнеры говорят:

«Как малый бизнес, мы не обладаем такими неограниченными ресурсами, как крупные игроки, поэтому мы ценим все, что дает нам преимущество. На одну вещь меньше, о которой нужно думать, на одну меньше расходы и одной заботой меньше».

Кроме того, АНБ работало с Управлением малого бизнеса Министерства обороны США, чтобыобеспечить, чтобы малые предприятия, принадлежащие меньшинствам, были осведомлены об этих услугахи иметь возможность использовать их для экономии средств и повышения безопасности сети.

Программа Enduring Security Framework (ESF) в сотрудничестве с 17 государственными и 62 отраслевыми партнерами выпустила 6 продуктов безопасности, направленных на устранение угроз в секторах критической инфраструктуры связи, DIB и информационных технологий. В частности, продукты ESF направлены на устранение угроз, связанных с 5G, управлением идентификацией и доступом, а также цепочкой поставок программного обеспечения. В этих выпусках содержались эффективные рекомендации и устанавливались лучшие отраслевые практики по смягчению выявленных угроз.

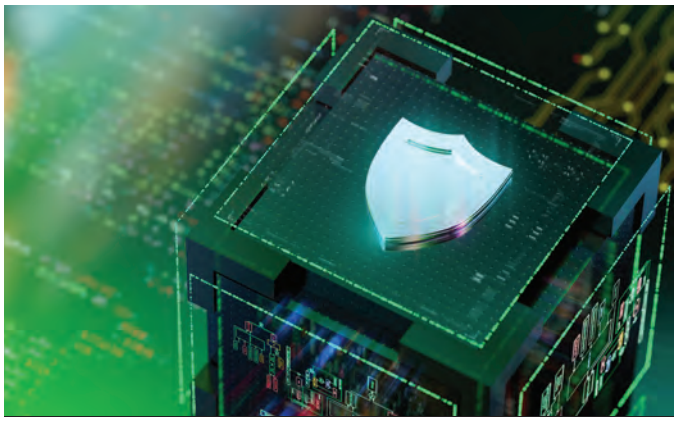


Фото предоставлено Getty Images

- Обеспечение безопасности цепочки поставок программного обеспечения: рекомендуемое практическое руководство для поставщиков
- Обеспечение безопасности цепочки поставок программного обеспечения: рекомендуемое практическое руководство для клиентов
- Потенциальные угрозы нарезке сети 5G
- Рекомендуемые рекомендации для администраторов: управление идентификацией и доступом
  - »Управление идентификацией и доступом Образовательные Помощь и связанные с ней темы для разговора
- Нарезка сети 5G: соображения безопасности при проектировании, развертывании и обслуживании

Масштабирование услуг кибербезопасности DIB

В этом году АНБ также обогатило свои предложения, используя уникальные знания АНБ о кибератаках национальных государств. Ярким примером является служба Защитной системы доменных имен (PDNS) АНБ, которая блокирует пользователям подключение к известным вредоносным или подозрительным веб-сайтам. АНБ разработало специальный канал угроз для PDNS, с помощью которогоАНБ предоставляет сотни уникальных индикаторов компрометации (IOC) еженедельно.своему поставщику DNS-фильтрации, чтобы они могли обновить свой черный список. Эти IOC получены из трех источников:

1. Данные SIGINT АНБ,
2. Аналитика АНБ, или
3. По совету межведомственных, отраслевых или международных партнеров.

На сегодняшний день АНБСервис PDNS сгенерировал 10 миллиардов блоков для участвующих клиентов.Из них 20 миллионов блоков получены по индикаторам, предоставленным АНБ, то естьАНБ препятствует возникающей вредоносной кибератаке, которая в противном случае осталась бы незамеченной и непреодолимой.Эти МОК также передаются правительству США и международным партнерам для обеспечения защитных действий.

В этом году АНБ также улучшило своюпрограмма сканирования уязвимостей, предлагающая комплексную поддержку управления поверхностями атак.Эта программа предлагает два существенных преимущества для предприятий DIB. Во-первых, он использует инструменты с открытым исходным кодом, чтобы предоставить компаниям полный перечень их интернет-активов, поскольку Вы не можете защитить то, о чем не знаете.Затем эта программа выполняет сканирование уязвимостей в этих активах и предоставляет индивидуальный отчет.

с уязвимостями в приоритете, используя знания АНБ о том, чем эксплуатируют субъекты национальных государств.

Новинкой этого года АНБ также запустило функцию «непрерывного мониторинга». Каждый день АНБ отслеживает различные источники, чтобы увидеть, когда субъекты национальных государств начинают использовать общеизвестные уязвимости. Когда уязвимость переходит от «известной» к «эксплуатируемой», АНБ немедленно осуществляет поиск в своем реестре обнаружения активов, чтобы определить, какие клиенты DIB могут иметь эту уязвимость в своей среде, и сигнализирует им об активной эксплуатации устройства, которое присутствует в их среде. среда. Эти уведомления получают отклик в 80% случаев и доказывают, что в результатекомпании находят и устраняют проблемы до компрометации и кражи данных.

В этом году программа управления поверхностями атак помогла раскрыть масштабную кампанию, связанную с Китайской Народной Республикой, направленную против нескольких компаний DIB, используя уязвимость в средах Citrix. В результате сотрудничества АНБ с крупными и малыми компаниями DIB и Cisco, АНБ публично разоблачило эту кампанию вместе с выпуском исправления. Независимые исследователи опубликовали блоги, отметив, что через несколько дней после публикации рекомендаций количество уязвимых серверов в США и странах-союзниках сократилось почти на 25%.

АНБслужба совместной работы по анализу угрозповзрослел в этом году. Благодаря этой услуге компании могут получать закрытую информацию об угрозах АНБ, специфичную для DIB, через безопасный, несекретный канал сотрудничества. Этот метод дает компаниям доступ к аналитическим возможностям АНБ, просто открыв приложение на своем телефоне, увеличивая их возможности и способность принимать меры и лучше защищать свои сети и сети своих клиентов.

Увеличение числа инновационных пилотов

Инвестиции в услуги кибербезопасности DIB на этом не закончились. В этом году АНБ запустило четыре новых пилотных проекта, которые продлятся 12 месяцев и проверят, эффективна ли служба в смягчении активности национальных государств, является ли она недорогой и масштабируемой без значительных накладных расходов для участвующих компаний. Новые пилоты:

- Облачная безопасность:Поскольку облачные вычисления быстро становятся нормой кибербезопасности, АНБ концентрирует усилия на обнаружении и устранении уязвимостей и неправильных конфигураций в DIB, которые делают их сети и интеллектуальную собственность уязвимыми. Этот пилотный проект также предоставит аналитикам CCC АНБ данные, необходимые для понимания поверхности облачных атак DIB, которые будут использоваться для разработки и распространения руководств по облачной безопасности, специфичных для DIB.

- Охота за угрозами:Выявление и устранение угроз до того, как они причинят вред, предполагает активное предоставление партнерам DIB платформы системной информации и управления событиями, чтобы облегчить обнаружение и смягчение вредоносной и подозрительной сетевой активности. Аналитики АНБ будут заниматься охотой вместе с партнерами DIB и разработают руководства и аналитику по поиску угроз для распространения по всему DIB.

- Защита от фишинга:Фишинговые атаки широко распространены. Этот пилотный проект предоставляет клиентам DIB безопасный шлюз электронной почты для фильтрации фишинговых атак, а также доступ к «песочнице», позволяющей лучше понять любое вредоносное ПО, связанное с вредоносными вложениями, и обеспечить соответствующую разработку средств защиты.

- Автономное тестирование на проникновение:В этом пилотном проекте новаторски используются автоматизированные инструменты, алгоритмы и искусственный интеллект для более непрерывного выявления цифровых уязвимостей, чем возможности человека. Имитируя действия хакеров, это тестирование обеспечивает оценку угроз в режиме реального времени, чтобы уменьшить вмешательство человека, повысить эффективность и предоставить более глубокое представление о том, как думают наши злоумышленники.

В цифрах

750
Партнеры

10Б
Блокировка вредоносных/подозрительных доменов, в том числе программ-вымогателей и вредоносного ПО национального уровня, целевого фишинга и ботнетов.

100 с
О новых уникальных MOK, которые еженедельно попадают в черный список АНБ

20M
Созданные блоки из уникальных MOK АНБ

312 000
Активы, подключенные к Интернету, идентифицированы и инвентаризированы для участвующих компаний DIB

1,3 млн.
Обнаружены и отмечены уязвимости, требующие исправления.

550+
Уязвимость партнера
Уведомления отправлены, процент ответов составляет 80 %.

70
Уникальные группы известных действий национальных государств, постоянно отслеживаемые АНБ и промышленностью.

Несколько
Обнаружены кампании национальных государств, нацеленные на DIB, в том числе те, которые используют уязвимости нулевого дня

Защита искусственного интеллекта (ИИ)

Новый Центр безопасности искусственного интеллекта АНБ, расположенный в Центре сотрудничества в области кибербезопасности, будет продвигатьбезопасная разработка, интеграция и внедрение возможностей искусственного интеллектав рамках систем национальной безопасности и DIB. Этот центр также будет использовать уникальные данные АНБ по внешней радиоразведке, чтобы помочь отрасли понять, как злоумышленники используют ИИ и нацелены на него. Привлекая лидеров промышленности США, национальных лабораторий и научных кругов совместно с разведывательным сообществом, Министерством обороны и иностранными партнерами, Центр безопасности ИИ поможет разработать передовые методы и рекомендации по обеспечению безопасности ИИ.

Партнерство для борьбы с угрозами и установления стандартов

Центр стандартов кибербезопасности (CCSS) занимается разработкой, информированием и внедрением стандартов телекоммуникаций, уделяя особое внимание обеспечению безопасности 5G и подготовке протоколов для квантовостойкой криптографии. На сегодняшний день CCSS разработал и представил более 95 стандартов для 5G, облачных сетей и интернет-протоколов. Эта работа обеспечивает встроенную безопасность и снижает возможности наших противников украсть интеллектуальную собственность США.АНБ участвует в работе более чем 15 организаций по разработке стандартов и более чем 40 рабочих групп. АНБ поддерживало правительство США, предоставляя техническую экспертизу на различных форумах. На форуме сектора электросвязи Международного союза электросвязи CCSS выступал в качестве исполняющей обязанности делегации США, работая в тесном партнерстве с Государственным департаментом. CCSS разработал несколько проектов стандартов безопасных протоколов в Инженерной рабочей группе Интернета, чтобы обеспечить постквантовую устойчивость и функциональную совместимость.

CCSS АНБ теперь является членом Альянса открытых сетей радиодоступа (O-RAN), международного консорциума, который разрабатывает стандарты сетей радиодоступа (RAN) для 5G. Альянс O-RAN исторически был закрыт для участия правительства США и раньше больше ориентировался на рыночные стимулы, чем на требования безопасности. Поскольку технология RAN лежит в основе инфраструктуры 5G, участие в основанном на консенсусе альянсе O-RAN представляет собой способ для СШАспособствовать достижению целей безопасности для 5G.

В рамках структуры устойчивой безопасности CCSS завершил исследование, направленное на активизацию деятельности США. и сопутствующие инвестиции в организации по разработке стандартов (SDO), которые обеспечивали долгосрочную безопасность критически важных технологий. Группа оценила технические и геополитические угрозы международным ООЗ и разработала стратегии противодействия этим угрозам. АНБ и его правительство США, промышленность и международные партнеры повысили осведомленность об угрозах стандартам.

Фото предоставлено Getty Images

и разработать стратегию борьбы с этими угрозами.Лучший способ борьбы с иностранным враждебным влиянием в международных ООЗ — это предложить странам, разделяющим одни и те же ценности безопасности, конфиденциальности и глобальной рыночной конкуренции, предложения по технически обоснованным стандартам.

Коммерческие продукты все чаще используются для обеспечения безопасности систем национальной безопасности (НСБ). Через Национальную программу обеспечения информации (NIAP) ССС сертифицировано 57 коммерческих компонентов для защиты НСС. Кроме того, NIAP опубликовал 3 профиля защиты для повышения безопасности этих продуктов. Профили защиты — это независимые от поставщика рекомендации, которые повышают безопасность коммерческих продуктов путем определения минимальных требований к безопасности и тестированию. NIAP также готовится обновить профили защиты, чтобы они соответствовали рекомендациям коммерческого алгоритма национальной безопасности (CNSA) 2.0, многофакторной аутентификации и принципам нулевого доверия.

NIAP продолжал укреплять глобальную позицию ИТ-безопасности посредством постоянного партнерства с 31 страной в рамках Соглашения о признании общих критериев (CCRA). CCRA гарантирует согласованность оценок между членами и взаимное признание, что позволяет поставщикам протестировать один раз, а затем продавать в нескольких странах. Она позиционирует Соединенные Штаты как лидера мирового сообщества благодаря дальнейшему принятию своих стандартов и сертификации большего количества продуктов, чем любая другая страна в CCRA. НИАП продолжал возглавлять Управляющий комитет CCRA и организовывал сотрудничество в целях взаимного признания. НИАП также провел Международную конференцию по общим критериям и Совещание по общим критериям в Вашингтоне, округ Колумбия, на котором были представлены 26 стран, что еще раз подчеркнулоценность международного партнерства для следующего поколения коммерческих технологий.

Изображение сделано во время саммита «Угрозы стандартам».

АНБ организовало рабочую группу по операциям по обману вместе с партнерами из отрасли. Эта рабочая группа возникла благодаря успеху отраслевых партнеров в использовании ловушек и желанию наших партнеров поделиться другими инструментами и методами, связанными с операциями по обману. Партнеры по отрасли поделились своим опытом и объяснили различные подходы к операциям по обману, а эксперты АНБ предложили свои технические точки зрения. Рабочая группа создала открытый диалог для будущего сотрудничества между промышленностью и АНБ. изучить новые методы не только для защиты сетей от иностранных противников, но и узнать больше о развивающихся методах, которые злоумышленники используют для нападения на оборонно-промышленную базу, Министерство обороны и другую критически важную инфраструктуру США.

АНБ также продолжило сотрудничать с партнерами для установления стандартов кибербезопасности, проведя первый саммит «Угрозы стандартам», собрав вместе экспертов по стандартам из правительства США, иностранных партнеров, промышленности и научных кругов для изучения растущих проблем и рисков, связанных со стандартами кибербезопасности.

> Эти коллективные усилия уже привели к созданию дорожной карты для наших партнеров, которая обеспечит подотчетность и поможет нам всем продолжать совершенствоваться.
>
> Морган Адамски
>
> Руководитель Центра сотрудничества в области кибербезопасности

УСЛУГИ КИБЕРБЕЗОПАСНОСТИ АГЕНТСТВА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Снизьте риск, защитите информацию Министерства обороны

АНБ предлагает компаниям с активным контрактом Министерства обороны (суб- или основным) или с доступом к закрытой информации Министерства обороны несколько решений по кибербезопасности с учетом угроз, которые помогут снизить риск компрометации сети и защитить конфиденциальную, но несекретную информацию.

Преимущества

Получите информацию об угрозах АНБ

Партнерство с АНБ по вопросам непубличной

Информация об угрозах АНБ,

специфичная для DIB

Улучшите защиту сети

Наши услуги помогут повысить безопасность ваших сетей

Получите руководство по смягчению последствий

Мы предоставляем рекомендации по устранению уязвимостей

Взаимодействуйте конфиденциально

Все партнерские отношения подкреплены соглашениями о неразглашении информации.

ШМ

Наше мнение

задницы

И в

Успех в цифрах

- Заблокировано**1Б**мгновенно через Защитный
- Идентифицировано**более полудня**
- Обнаруженный**более 8**
- Идентифицировано**более 20**
- Идентифицировано**почти 7**

НАШ СЕР

Поддержка CMMC — NIST 800-171 Оценка рисков 3.11.02, 3.11.03

Сотрудничество в области анализа угроз

Сотрудничайте с АНБ, чтобы получать закрытую информацию об угрозах, специфичную для DIB.

возможность участвовать в совместно используемых материалах.

выявляли, выявляли и устраняли попытки активной эксплуатации сотен зарегистрированных клиентов.

rt — NIST 800-171 Целостность системы и информации 3.14.03

ов/ссс

терия

нт

Отзыв отраслевого партнера:

Благодарим вас за вашу поддержку во время плавной интеграции пакета кибербезопасности АНБ для оборонно-промышленной базы... В течение пятнадцати минут... мы были возможность настроить наш... брандмауэр для различных служб».

CYBERSECURITY COLLABORATION CENTER

Постановка на охрану

Чистые защитники под руководством

Обмен своевременными и действенными рекомендациями

У сетевых защитников много задач в современной сложной среде угроз, и им нужна своевременная информация для устранения значительных уязвимостей и защиты своих сетей от киберпреступных и злонамеренных угроз.

Публичные отчеты АНБ, которые часто публикуются при участии все большего числа сотрудников, помогают защитникам сетей получить рекомендации, необходимые для решения этих критических проблем кибербезопасности.

В координации с партнерами АНБ подготовило в этом году 27 рекомендаций по кибербезопасности и информационных листов по кибербезопасности для публичного выпуска. Эти отчеты, доступные на сайте NSA.gov, охватывают широкий спектр тем: от того, как лучше всего защитить домашние сети до того, как правительство Северной Кореи использует социальную инженерию для взлома аналитических центров, научных кругов и средств массовой информации.

Другой пример помогает организациямконтекстуализировать дипфейковые угрозы . Дипфейки — это созданные искусственным интеллектом высокореалистичные синтетические медиа, которыми можно злоупотреблять, чтобы поставить под угрозу бренд организации, выдать себя за лидеров и обеспечить доступ к сетям, коммуникациям и конфиденциальной информации. В сотрудничестве с ФБР и CISA АНБ выпустило информационный бюллетень по кибербезопасности «Контекстуализация дипфейковых угроз для организаций». В нем был представлен обзор синтетических медиа-угроз, методов и тенденций, а также рекомендации, рекомендации и стратегии смягчения, направленные на защиту организаций от развивающихся дипфейковых угроз.

Опубликовав это руководство публично, АНБ вместе с агентствами-соавторами сможет обеспечить важные шаги по смягчению последствий, чтобы помочь защитить ряд сетевых информационных систем.

АНБ также упростило выпуск индикаторов компрометации, связанных с различными типами вредоносных программ, с помощью автоматизированных отчетов Network Defense Notification (NDN). Эти NDN предоставляют партнерам сообщества быструю обновленную информацию об индикаторах компрометации, связанных с вредоносными программами, наблюдаемыми в дикой природе.они могут использовать их для предотвращения потенциального компрометации своих систем.

27 | Рекомендации по кибербезопасности

Информационные бюллетени и информационные бюллетени по кибербезопасности для публичного распространения

Защита

Наши наиболее важные сети

Защита ключевых систем

АНБ продолжает поддерживать реализацию «Меморандум об улучшении кибербезопасности систем национальной безопасности, Министерства обороны и разведывательного сообщества» ,известный как Меморандум национальной безопасности-8 (NSM-8).

Этот меморандум предоставил директору АНБ как национальному менеджеру по системам национальной безопасности (НСБ) новые полномочия, которые повысили прозрачность кибербезопасности АНБ в сетях, которые содержат секретную информацию или иным образом имеют решающее значение для военной и разведывательной деятельности в правительстве. С момента подписания NSM-8 АНБ установило еще более тесные отношения с более чем 50 департаментами и агентствами США, которые владеют или управляют НСС. АНБ продолжает повышать безопасность критически важных систем правительства США для защиты конфиденциальных военных и разведывательных данных от наших противников.

Защита национальных тайн

АНБ интегрировано в разработку и создание систем национальной безопасности и вооружений Министерства обороны США, а также их криптографии. АНБ продолжаетзащитите миллионы устройств по всему мируи управлять инфраструктурой для ключей этих устройств с помощью своих ключей, кодов и криптографии. Это включает производство и распространение ключей, кодов и криптографических материалов, которые используют правительство и военные США.для обеспечения безопасности оружия, спутников, связи и многих других систем, от которых критически зависит национальная безопасность.

АНБ отвечает за защиту самых важных секретов страны от наиболее способных противников страны, кибер-способных национальных государств и отдельных лиц, которые хотят проникнуть в наши сети или взломать наше шифрование.

Ключи, коды и криптография АНБ защищают все: от сертифицированных АНБ тактических радиостанций и любого зашифрованного оборудования, находящегося в руках американских солдат, моряков, летчиков, стражей и морской пехоты, до их критически важных оружейных платформ, включая системы ядерного управления и контроля. АНБгарантирует, что эти системы, которые используют наши военные, устойчивы к атакам кибербезопасности.и защитить стратегическое преимущество США в конфликте.

За последний год несекретные данные АНБАнализ инфраструктуры обфускации КНР позволил улучшить защиту систем национальной безопасности.Центр сотрудничества в области кибербезопасности выявил злонамеренную киберактивность, приписываемую КНР, посредством аналитических методов, используя несекретные каналы коммерческих разведывательных данных об угрозах. Автоматизированное создание отпечатков пальцев датчиков на основе этого метода упростило идентификацию действий КНР в отношении сетевой структуры систем национальной безопасности.

Безопасность операционных технологий

Киберпреступники готовы осуществлять вредоносную кибердеятельность против критической инфраструктуры, используя доступные через Интернет и уязвимые активы операционных технологий (ОТ). АНБ провело оценку многочисленных сайтов Министерства обороны, выпустило несколько рекомендаций по кибербезопасности и уведомлений о защите сети для обеспечения безопасности ОТ и продолжает обеспечивать безопасность инфраструктуры ОТ и систем национальной безопасности. С этой целью АНБ предоставило на CyberGitHub АНБ хранилище сигнатур и аналитики для обнаружения вторжений ОТ. Эта возможность, известная как ELITEWOLF, может позволить защитникам критической инфраструктуры, оборонно-промышленной базы и систем национальной безопасности выявлять и обнаруживать потенциально вредоносную киберактивность в своих ОТ-средах.

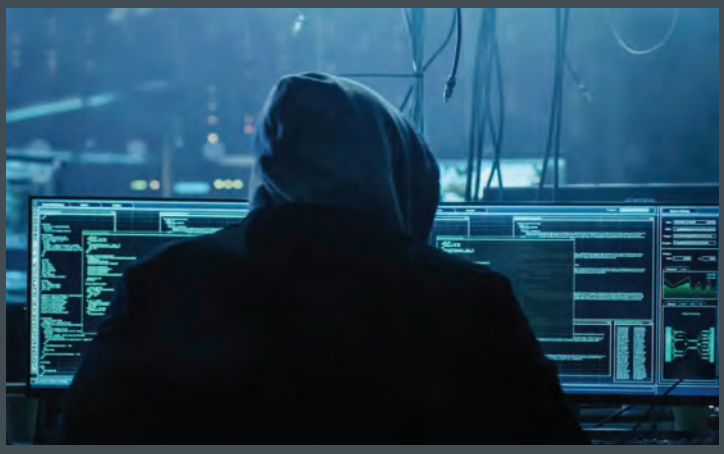
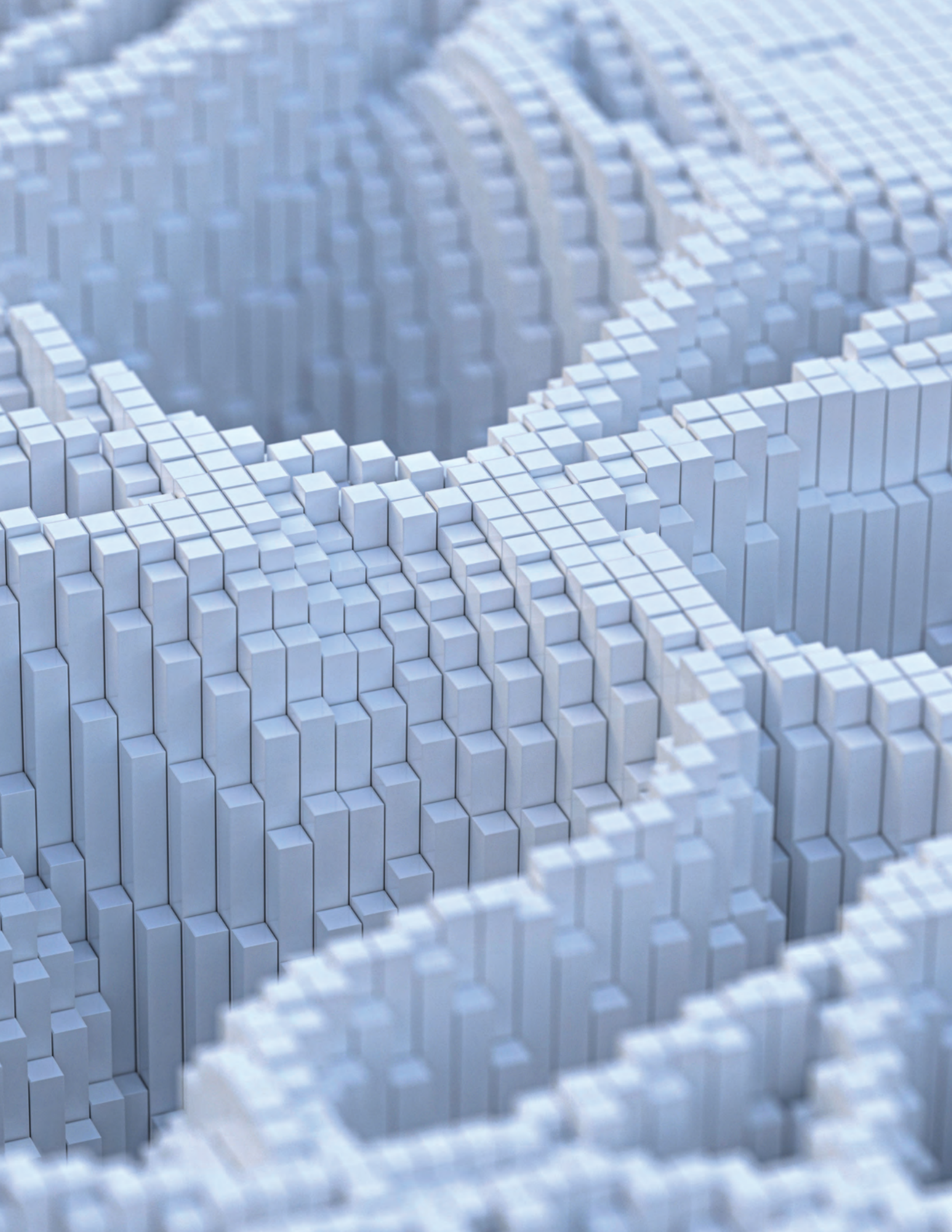


Фото предоставлено Getty Images


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
CYBERSECURITY



Модернизация

Криптографические решения для защиты данных и коммуникаций

Прогресс в направлении

Квантовая криптография

Когда это будет достигнуто, криптоаналитически значимый квантовый компьютер изменит игру. Он создаст угрозу наиболее важным информационным системам нашей страны и разрушит криптографические системы, обеспечивающие безопасность Интернета и информационных систем по всему миру.

Квантовоустойчивая криптография по-прежнему остается лучшей защитой от этой надвигающейся угрозы.

АНБ продолжает стратегически осуществлять национальную безопасностьМеморандум-10 (НСМ-10) , «Продвижение лидерства США в области квантовых вычислений при одновременном снижении рисков для уязвимых криптографических систем», который предписывает правительственным учреждениям США перевести уязвимые криптографические системы на квантовостойкую криптографию, что представляет собой многолетний переход.

В качестве национального менеджера по системам национальной безопасности (NSS) директор АНБ курирует переход к квантовостойкой криптографии в более чем 50 правительственных ведомствах и агентствах, использующих NSS.

Продолжающееся партнерство и сотрудничество с правительством и частными партнерами является ключом к решению этой проблемы кибербезопасности. АНБ сотрудничает с Национальным институтом стандартов и технологий (NIST) — руководителем утверждения коммерческих алгоритмов правительства США — а также с Агентством кибербезопасности и безопасности инфраструктуры (CISA), Управлением директора национальной разведки, науки и технологий (ODNI S&T). , Министерство обороны и внешние организации по стандартизации.

Сообщество кибербезопасности, включая промышленность, правительство и научные круги, должно уже сейчас планировать модернизацию криптографии.Квантовые вычисления, возможно, не кажутся непосредственной угрозой, но это надвигающаяся угроза, против которой необходимо принимать меры уже сейчас.

В прошлом году АНБ опиралось на ранее опубликованный пакет Commercial National Algorithm Suite 2.0, который уведомил владельцев, операторов и поставщиков НСС о будущих требованиях к квантово-устойчивым алгоритмам для использования во всех НСС. В марте и июне АНБ выпустило руководство, призванное помочь правительству США выявлять и инвентаризировать квантовые уязвимой криптографии, укрепить текущий набор криптографии иплан перехода к квантовостойкой криптографии.Переход к этой модернизации включает в себя инвентаризацию криптографии, определение приоритетов, планирование и применение ресурсов для усилий по квантовой устойчивости, а также планирование внедрения набора квантовоустойчивых алгоритмов АНБ и криптографических стандартов NSS и NIST.

> “Постквантовая криптография предполагает активную разработку и создание возможностей для защиты критической информации и систем от компрометации с помощью квантовых компьютеров. Переход к эпохе безопасных квантовых вычислений — это долгосрочная интенсивная работа сообщества, требующая широкого сотрудничества между правительством и промышленностью. Главное — отправиться в это путешествие сегодня, а не ждать до последней минуты.
>
> Роб Джойс,
> Директор АНБ по кибербезопасности

Переход к квантовостойкой криптографии — лишь один из примеров того, как АНБ остается на шаг впереди противников нашей страны в защите наших самых конфиденциальных данных. АНБ постоянно модернизирует свои решения в области кибербезопасности, чтобы они были гибкими, адаптируемыми к угрозам и масштабируемыми для многодоменных операций.

Фотография ВМС США, сделанная специалистом по массовым коммуникациям
3-й класс Николас В. Хюин

550

Устройства COMSEC

Быстрое развертывание

234 415

Индикация несанкционированного доступа

Доставленная продукция

Глобально

61

Уникальные клиенты

Поддерживается для критических

Операции

20+

Кибер-столешница

Упражнения и техника

Обмен встречами

Защита

Боец и поддерживающие боевые команды

Поддержка армии

В рамках Министерства обороны АНБ является агентством боевой поддержки и поддерживает военные службы, выполняя две ключевые задачи: иностранную радиоразведку и кибербезопасность. В то время как эксперты по внешней радиоразведке АНБ оказывают разведывательную поддержку военным операциям, его эксперты по кибербезопасности помогают обеспечить безопасность военных коммуникаций и данных.

АНБ развивало прочное партнерство с Киберкомандованием США, оказывая поддержку Оперативные операции по охотепри этом команды развертываются по всему миру по просьбе наших партнеров, чтобы помочь им в борьбе со злонамеренными киберпреступниками.

Военные должны быть уверены в своих действиях. Вклад АНБ помогает именно в этом, так что американские военные имеют возможность обеспечивать связь для таких операций, как ядерное командование и контроль, и различать друзей и врагов. Вместе с правительственными партнерами АНБ помогает обеспечить безопасность ключевых функций управления, сетей, систем и коммуникационных устройств, используемых Министерством обороны. АНБ также предоставляет передовые методы обеспечения безопасности связи, чтобы гарантировать безопасную обработку криптографических материалов, используемых в этих системах и устройствах.

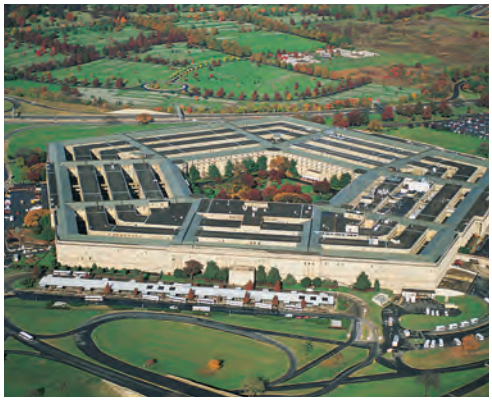
АНБ также предоставляет продукты криптографической безопасности для удовлетворения незапланированных чрезвычайных потребностей и поддержки срочных миссий. За последний год АНБ быстро развернуло около550 устройств безопасности связи (COMSEC)для поддержки операций миссии во время глобальных кризисов ипоставлено 234 415 изделий, сигнализирующих о несанкционированном доступево всем мире в 2023 году. Продукты с индикацией несанкционированного доступа предотвращают или обнаруживают физическую эксплуатацию криптографического оборудования и секретных материалов во время транспортировки или развертывания по всему миру.

В прошлом году АНБ продолжалоподдержка 61 уникального клиента для критически важных операций такие как Индо-Тихоокеанское командование США, Европейское командование США, Объединенный комитет начальников штабов, Транспортное командование США, Национальное управление по аэронавтике и исследованию космического пространства (НАСА), Федеральное агентство по чрезвычайным ситуациям (FEMA) и многие другие.

АНБ приняло участие вболее 20 кибер-кабинетных учений и встреч по техническому обмену В результате было подготовлено 7 отчетов об оценке уязвимостей с планами смягчения последствий и рекомендациями по инженерной безопасности. АНБ продолжает оказывать помощь в разработке стратегий оборонительного мониторинга, помогающих улучшить ситуационную осведомленность оружейных платформ.

АНБ также в партнерстве с Агентством космического развития (SDA) разработало космическую архитектуру для боевых действий, которая позволила SDA успешно запустить свои первые десять спутников, ознаменовав новую эру в национальной обороне.

Кроме того, АНБ участвовало в многочисленных брифингах и обсуждениях с руководством и персоналом Космического командования США. АНБ предоставило сотрудникам Космического командования США информацию о предложениях услуг по кибербезопасности и деловой практике, используемой Центром сотрудничества в области кибербезопасности для инициирования и развития отношений с отраслевыми партнерами. Участники Космического командования США также кратко рассказали о развитии коммерческих отношений Космического командования США. Это партнерство будет способствовать дальнейшему расширению партнерских отношений Центра сотрудничества в области кибербезопасности среди ключевых партнеров Космического командования США.



Как описывалось ранее, все сообщество кибербезопасности должно уже сейчас планировать модернизацию шифрования и предотвращение надвигающейся квантовой угрозы. В прошлом году АНБ продолжило свои усилия помодернизировать шифрование в боевых командованиях США.Сотрудничая с Киберкомандованием США и штабом объединенных сил и информационными сетями Министерства обороны, АНБ снижает вероятность того, что противники США смогут получить доступ к средствам связи военных и конфиденциальным данным.

Совместная мониторинговая деятельность COMSEC (JCMA) продолжала выявлять утечку важных деталей военных операций и информации о поездках высокопоставленных лиц, обнаруженную в несекретных сообщениях, которая может увеличить риски для миссий и персонала. JCMA направила боевым командованиям отчеты о действиях и исправлениях в связи с этими выводами.

Оценка систем и создание дорожных карт

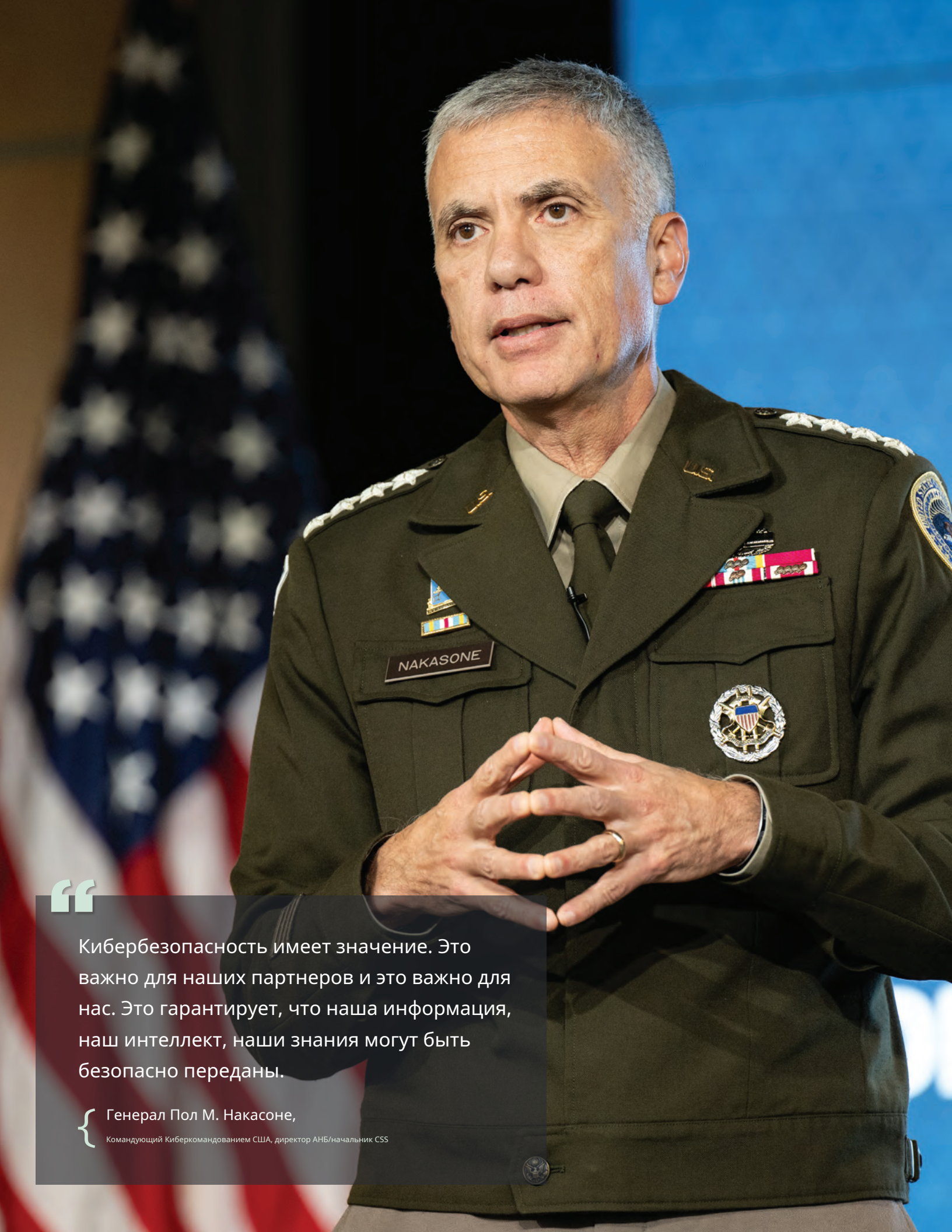
Проведение критическихоценки кибербезопасности некоторых наиболее важных вооруженных и космических систем страны.во всех областях боевых действий помогает гарантировать, что они не уязвимы для киберпреступников. АНБ продолжало эту важную работу в течение прошлого года.

В 2023 году агентствозавершенные криптографические дорожные карты для каждого боевого командования СШАпартнер по коалиции. АНБ использовало заседания Совета по взаимодействию командования и управления между боевыми командованиями США и их партнерами для определения критических миссий с использованием устаревшей криптографии и прямой модернизации, ориентированной на выполнение миссии. платформы для поддержки миссии. Эти усилия определяют, куда необходимо направить ресурсы, чтобы гарантировать безопасность партнеров от передовых киберугроз во всех сферах боевых действий и полную совместимость с силами США и их союзников.

Фотографии любезно предоставлены Getty Images

В рамках программы стратегической кибербезопасности Министерства обороны АНБ работало совместно с руководителями Министерства обороны и военными службами США, чтобыоценить свои системы и разработать планы по устранению уязвимостей, модернизации криптографии и мониторингу систем. В будущем АНБ планирует расширить эту деятельность за счет дальнейшего сотрудничества с военными службами для проведения дополнительных оценок кибербезопасности приоритетных систем. АНБ также предоставило оперативныеподдержка военных учений и планирование конференций.

АНБ продолжает организовывать и осуществлятьоценки рисков кибербезопасности наиболее важных систем Министерства обороны, помогая Министерству обороны обеспечить дальнейшее совершенствование и укрепление его систем перед лицом постоянных и стойких киберугроз. В течение прошлого года АНБ предоставило обзоры Zero Trust и планы внедрения двух критически важных систем для ВМФ и ВВС. Эта продукция стала результатом длительного сотрудничества с ВМФ и ВВС на протяжении всего года.



> Кибербезопасность имеет значение. Это важно для наших партнеров и это важно для нас. Это гарантирует, что наша информация, наш интеллект, наши знания могут быть безопасно переданы.

{ Генерал Пол М. Накасоне,

Командующий Киберкомандованием США, директор АНБ/начальник CSS

Помощь в совместимых миссиях

АНБ продолжает представлять США в группе НАТО по обеспечению информационной безопасности и возможностям киберзащиты, укрепляя отношения со странами-партнерами и уделяя особое внимание модернизации платформ и оборудования для оказания помощи.совместимые миссии.Поскольку США продолжают модернизировать криптографию, АНБ делится передовой криптографической логикой со способными партнерами НАТО, чтобы помочь модернизировать предприятие и альянс НАТО. В этом году АНБ подчеркнуло работу NIST по разработке возможностей квантовой устойчивости. Группа разрабатывает технические рекомендации и обмен информацией о кибербезопасности в рамках НАТО для защиты критически важных сетей от современных киберугроз.

Содействие кибербезопасности ядерного командования, контроля и связи (NC3)

В 2023 году АНБ продолжило сотрудничать с агентствами Министерства обороны в целях предотвращения и искоренения киберугроз системам ядерного командования и контроля, сосредоточив усилия на укреплении и развитии партнерских отношений. Эти отношения будут иметь решающее значение для расширения практики кибербезопасности и использования инновационных успехов.

При поддержке ключевого партнера, Стратегического командования США, АНБ предоставило прототип возможностей для использования датчиков и мониторинга, а также предоставило визуализацию для более глубокого понимания деятельности предприятия ядерного командования, контроля и связи (NC3). АНБ продолжит использовать большие данные для принятия решений, которые укрепят системы и искоренят угрозы.

АНБ также установило новые и укрепило существующие партнерские отношения для проведения оценок стратегической программы кибербезопасности NC3, включая риски кибербезопасности, планы смягчения последствий и рекомендации по защитному мониторингу для развернутых систем. Оперативная поддержка в этом году во время учений предоставила партнерам Министерства обороны реальные примеры того, как предотвращать и искоренять угрозы оружию и космическим системам.

Обеспечение безопасности NSS с помощью коммерческих решений

Программа АНБ «Коммерческие решения для секретной информации» (CSfC) позволяет клиентамСложные коммерческие решения для защиты секретной информации.Пакеты возможностей CSfC защищают НСС, предлагая надежный системный подход для военных служб США, боевых командований и других федеральных партнеров.

CSfC позволяет клиентам быстро настраивать и развертывать безопасные решения кибербезопасности, используя предварительно одобренные АНБ конструкции системного уровня и коммерчески доступные компоненты для удовлетворения широкого спектра сценариев использования в миссиях - не только внутри и между защищенными объектами, но также для обеспечения удаленного доступа для удаленной работы и работы. это происходит за пределами стандартных рабочих пространств.

В 2023 году CSfC продолжила совершенствовать и обновлять свои общедоступные пакеты возможностей, которые помогают клиентам внедрять собственные решения. В этом году CSfC опубликовала дополнительное руководство, созданное для устройств тонких конечных пользователей и закрытых ключей.

АНБ также обеспечивает гарантию полевых решений для таких клиентов, как ФБР, и других критически важных систем. CSfC провела оценку регистрации четырех клиентов CSfC на месте, в ходе которой зарегистрированное решение сравнивается с тем, что фактически было предложено внедряющей организацией. АНБ обеспечило соответствие конфигураций, мониторинга и администрирования требованиям пакета возможностей CSfC. Это дает возможность взаимного обогащения и обмена технологиями, одновременно используя возможности для повышения безопасности и ясности требований. АНБ планирует продолжить подобные оценки в будущем.

Фото предоставлено Getty Images

Фото предоставлено Getty Images

исследование

Решения по кибербезопасности

Лаборатория передовых исследований в области кибербезопасности АНБ остается на переднем крае защиты и обеспечения безопасности киберэкосистемы нашей страны благодаря надежным и процветающим партнерским отношениям с академическими учреждениями, исследовательскими лабораториями, финансируемыми из федерального бюджета, и частным сектором. АНБ имеет уникальные возможности для привлечения технического опыта мирового уровня для поддержки общегосударственных усилий по обеспечению устойчивого преимущества Соединенных Штатов в области искусственного интеллекта и машинного обучения. Ученые, инженеры и идейные лидеры АНБ в течение многих лет возглавляли и продвигали исследования, навыки и возможности в области науки о данных, и наш профильный опыт будет задействован для обеспечения безопасной разработки, интеграции и внедрения возможностей искусственного интеллекта в национальном масштабе США. Системы безопасности и оборонно-промышленная база.

Другие недавние достижения в области исследований в области кибербезопасности включают в себя:

- Укрепление стандартов кибербезопасности в будущих технологиях и форумах, имеющих решающее значение для страны, таких как Проект партнерства третьего поколения, который выступает в качестве ведущей организации по стандартизации 5G.
- Предоставление базовых рекомендаций по цепочке поставок защитникам сетей систем национальной безопасности и оборонно-промышленной базы, обеспечивающих целостность таких устройств, как настольные компьютеры, серверы и ноутбуки, участвующих во всех закупочных операциях на предприятии.
- Завершается последняя версия программы АНБ «Наука безопасности», которая способствует фундаментальным исследованиям в области кибербезопасности в академических учреждениях в области передовой науки и новейших технологий, и начинается следующая версия, спонсирующая серию новых проектов в семи различных университетах. Программа «Наука безопасности» приглашает к сотрудничеству академические круги, промышленность и правительство для продвижения кибербезопасности посредством научной строгости.
- Разработка курсов кибероператоров, призванных вооружить следующее поколение киберпрофессионалов передовыми навыками для оценки уязвимостей программного обеспечения и защиты наших национальных киберактивов.


ЖЕНЩИНЫ
погруженный
в АНБ
по кибербезопасности

Разработка

Нынешнее и следующее поколение киберэкспертов

Расширение кибертрудовых ресурсов

При поддержке Управления национального кибер-директора Белого дома АНБ в партнерстве с другими федеральными агентствами разработало и опубликовало первый в истории Национальная стратегия кибертрудовых ресурсов и образования,одобрен администрацией Байдена-Харриса в июле. Эта стратегия была разработана с учетом компонента, ориентированного на людей, в дополнение к Национальной стратегии кибербезопасности, подписанной президентом Байденом в марте, и включает четыре ключевых направления:

- Обеспечьте каждого американца базовыми кибернавыками
- Трансформируйте киберобразование
- Расширьте и улучшите кибер-рабочую силу
- Укрепление федеральной кибер рабочей силы

Стратегия была разработана при консультациях с промышленностью, научными кругами, некоммерческими организациями и государственными партнерами. АНБ внесло свой вклад в разработку стратегии и участвовало в рабочих группах Белого дома, уделяя особое внимание усилиям по киберобразованию и федеральным киберспециалистам. Обязательства АНБ включают пилотную инициативу по развитию «кибercлиник» по всей стране, которые будут поддерживать сообщества и небольшие правительства, которые в противном случае не имели бы доступа к оценке киберрисков и помощи в планировании. Клиники также предоставят возможность более чем 200 студентам развивать компетенции, находясь в контролируемой учебной среде.

Привлечение внимания и привлечение женщин в сферу кибербезопасности

Центр сотрудничества в области кибербезопасности АНБ вместе с академическими, промышленными и правительственными партнерами возглавляет работу по поощрению большего числа женщин к карьере в сфере кибербезопасности.

После успешного прошлогоднего пилотного проекта «Женщины, погруженные в кибербезопасность АНБ» (WIN-Cyber), пять новых школ и двадцать активных студентов приняли участие в WIN-Cyber '23, организованном в Центре сотрудничества в области кибербезопасности.

Программа WIN-Cyber — это недельный захватывающий процесс обучения, который позволяет студентам сотрудничать и учиться у некоторых ведущих специалистов по кибербезопасности АНБ и Киберкомандования США. Участники WIN-Cyber '23 были номинированы своими профессорами и представляли школы, в том числе двухгодичный общественный колледж, исторически черный колледж и университет, латиноамериканское обслуживающее учреждение и четырехлетний государственный университет. Студенты узнали о миссии АНБ по кибербезопасности, и многие вернулись в свои школы в качестве «послов» АНБ, которые выступают за общественную службу в своих кампусах.

Фотография сделана на мероприятии WIN-Cyber '23

Партнерство с академией

АНБ продолжает реализовывать свою академическую стратегию в области кибербезопасности, чтобы вдохновлять кибервоинов завтрашнего дня посредством таких инициатив, как:

The Задача по взлому кодов АНБпредоставляет студентам, посещающим академические учреждения США, возможность отточить свои кибернавыки и получить опыт работы в реалистичных сценариях, ориентированных на выполнение задач АНБ. До 21 декабря студенты работают над интерпретацией и обнаружением сигналов неизвестного происхождения, выявленных Береговой охраной США. Студентам предлагается серия из девяти все более сложных задач: найти и проанализировать причину, вызвавшую сигнал, обнаружить активную операцию сбора данных, порученную мошенническому серверу, и взломать мошеннический сервер, чтобы остановить устройство сбора.

TheГенКиберПрограмма предлагает круглогодичное обучение кибербезопасности для учащихся и преподавателей средней школы. Эта ежегодная конкурсная программа предлагается образовательным учреждениям, а также некоммерческим и некоммерческим учреждениям через академические учреждения. Претенденты могут подать заявку на четыре типа программ: студенческие, преподавательские, комбинированные и студенческие языковые. В 2023 году было профинансировано 160 программ в 47 штатах, а также в округе Колумбия и Пуэрто-Рико, в которых приняли участие около 5300 студентов и преподавателей. АНБ и Национальный научный фонд делают это возможным.

The Киберучения АНБ (NCX)развивает будущих военных и гражданских кибервоинов и лидеров, развивая и проверяя их навыки кибербезопасности, командную работу, планирование, общение и принятие решений. Эти ежегодные учения являются конкурентным киберсобытием года для Военных академий США, старших военных колледжей и участников программ профессионального развития АНБ. ВВС США были награждены трофеем NCX 2023.

Фотография сделана на мероприятии NCX 23'.

The Экспериментальный тур АНБобеспечивает четырех-шестинедельные туры в рамках АНБ, Киберкомандования США и партнеров почти в 200 академий обслуживания, Старшего военного колледжа и избранных членов Корпуса подготовки офицеров запаса (ROTC). Эти туры предоставляют как секретный, так и несекретный опыт, позволяя участникам формировать миссию, готовясь взять на себя руководящие роли.

Продвижение изучения кибербезопасности

АНБ инвестирует в продвижение карьеры в области кибербезопасности на всех уровнях образования. АНБ Национальный криптологический университет управляет Национальными центрами академического мастерства в области кибербезопасности (NCAE-C). Программа создает и управляет совместной образовательной программой по кибербезопасности с местными колледжами, колледжами и университетами, которая:

- Устанавливает стандарты учебных программ по кибербезопасности и академических успехов.
- Включает развитие компетенций среди студентов и преподавателей.
- Ценит работу с сообществом и лидерство в профессиональном развитии
- Интегрирует практику кибербезопасности внутри учреждения и между академическими дисциплинами.
- Активно участвует в решении проблем, стоящих перед образованием в области кибербезопасности.

Более 400 школ получили обозначение NCAE-C в области кибербезопасности, киберзащиты и кибериссследований.

Фотография предоставлена Getty Images.