HM Government

Национальная киберстратегия 2022

Прокладывая путь к кибербудущему вместе со всей Британией

Национальная киберстратегия 2022

Прокладывая путь к кибербудущему вместе со всей Британией

Содержание

Дополнительное содержание

Предисловие

Соединенное Королевство — открытое демократическое общество, богатый опыт сотрудничества и инноваций которого составляет основу нашего успеха как ориентированной на внешний мир глобальной нации. Это ярко продемонстрировали наши действия в ответ на чрезвычайные эпидемиологические ситуации глобального масштаба и усилия по достижению чистого нулевого уровня выбросов. Но наиболее ярко преимущества этого подхода проявились в киберпространстве.

Будь то реализация широкомасштабных преимуществ, которые киберпространство обеспечивает для наших граждан и экономики на фоне усилий по созданию равных условий и объединению в масштабах всей страны; объединение усилий с партнерами для построения киберпространства в соответствии с нашими национальными ценностями, или использование всего киберпотенциала для влияния на глобальные события, — Соединенное Королевство видит в кибертехнологиях средство, которое позволит защищать и продвигать наши интересы в условиях, формирующихся под воздействием технологического прогресса.

Новая национальная киберстратегия — это наш план, призванный обеспечить, чтобы Соединенное Королевство оставалось уверенным, жизнеспособным и устойчивым обществом в этом стремительно меняющемся цифровом мире и чтобы мы продолжали адаптироваться, внедрять инновации и вкладывать средства в возможности для защиты и продвижения наших интересов в киберпространстве.

Продолжая с того, на чем остановилась новаторская Национальная стратегия кибербезопасности 2016 года, мы начинаем новую главу на пути к построению будущего, в котором Соединенное Королевство станет еще более устойчивым к кибератакам. Как ведущий министр, я четко отмечаю две ее ключевые цели: первая — укрепление наших позиций в сфере технологий, имеющих критическое значение для киберпотенциала, и вторая — ограничение зависимости от отдельных поставщиков или технологий из стран, власти которых не разделяют наши ценности.

Британская наука и техника будут движущей силой этих перемен, обеспечивая, чтобы киберпотенциал оставался национальным экономическим и стратегическим активом, чтобы наши технологии были более надежными и способными отражать атаки широкого спектра киберпротивников, возможности которых до недавнего времени находились в исключительном владении национальных государств.

Британское правительство обязалось выделить 22 млрд фунтов стерлингов на исследования и разработки и поставить технологии в центр планов по укреплению национальной безопасности. Мы все видели, каким преобразующим потенциалом обладают цифровые технологии, а также их разрушительные возможности, как например в случае 5G. Наши планы в области искусственного интеллекта и информационной политики помогут нам выйти на передовые позиции в использовании преимуществ этих технологий, а меры, принятые в рамках киберстратегии, помогут нам укрепить уверенность в безопасности и устойчивости поставщиков и партнеров.

Создание Национальных сил кибербезопасности в прошлом году представляет собой важный шаг в наращивании наступательного киберпотенциала. Однако наши усилия по по-прежнему сосредоточены на обеспечении базовой кибербезопасности, и мы ужесточаем нашу реакцию на действия тех, кто атакует Соединенное Королевство и наших граждан. Мы также сосредоточим усилия на повышении устойчивости государственного сектора, помогая местным советам обеспечивать защиту их систем и персональных данных граждан от атак программ-вымогателей и других кибератак.

Киберпространство — всеобщее достояние. Опираясь на эту стратегию, правительство прилагает больше усилий для защиты британских граждан и компаний и международных партнеров, обеспечивая реализацию своего видения киберпространства как надежной и устойчивой сферы, способствующей процветанию людей и компаний.

Достопочтенный Стив Баркли, член парламента, Канцлер герцогства Ланкастерского и министр кабинета министров

Введение

Возможности и вызовы цифровой эпохи

1. Стремительная эволюция технологий в сочетании со снижением затрат связали мир теснее, чем когда-либо, открывая уникальные возможности и активизируя инновации и прогресс. Пандемия коронавируса (COVID-19) ускорила эту тенденцию, но мы, по всей видимости, все еще находимся на ранних стадиях долгосрочного структурного сдвига. Глобальная экспансия киберпространства изменяет то, как мы живем, работаем и взаимодействуем, и трансформирует критически важные системы, на которые мы полагаемся в таких областях, как финансы, энергетика, распределение продовольствия, здравоохранение и транспорт. Иными словами, киберпространство стало неотъемлемым элементом нашей будущей безопасности и процветания. Это открывает перед такими технологически развитыми странами, как Соединенное Королевство, уникальные возможности для достижения своих целей новыми путями.

2. Масштабы и скорость наступления этих перемен — которые зачастую опережают развитие норм социальной жизни, законов и демократических институтов — также приводят к возникновению беспрецедентных сложностей, нестабильности и рисков. В прошлом году мы были свидетелями кибератак на больницы и нефтепроводы, школы и компании, и в некоторых случаях — полной парализации деятельности организаций в результате атак программ-вымогателей, а также использования шпионского ПО против активистов, журналистов и политиков. В силу транснациональной природы киберпространства эти вызовы невозможно преодолеть без международного сотрудничества, при этом киберпространство становится все более важной областью системного соперничества и столкновения конкурирующих интересов, ценностей и видений нашего общего будущего.

Наше видение: использование кибермощи для содействия достижению национальных целей

3. В этом контексте кибермощь становится еще более важным рычагом национальной мощи и источником стратегического преимущества. **Кибермощь — это способность защищать и продвигать национальные интересы в киберпространстве и с его помощью.** Страны, способные ориентироваться в многообразии возможностей и вызовов цифровой эпохи, будут более защищенными, устойчивыми и процветающими в будущем. Соединенное Королевство — одна из самых развитых в цифровом плане стран, и у текущего правительства есть амбициозная национальная и международная повестка дня в области технологий. Это означает, что мы сталкиваемся с особенно серьезными вызовами в киберпространстве, но вместе с тем располагаем уникальными возможностями, чтобы играть лидирующую роль в использовании его преимуществ на благо наших граждан и всего человечества.

4. В течение следующих десяти лет интернет, цифровые технологии и инфраструктура, лежащая в их основе, будут иметь еще более важное значение для обеспечения наших интересов и интересов наших союзников и противников. На фоне формирования новой роли Соединенного Королевства в эпоху обостряющегося соперничества укрепление кибермощи позволит нам проложить путь для отраслевых предприятий и других стран, предвосхищать будущие технологические изменения, смягчать угрозы и получать стратегические преимущества перед нашими соперниками и конкурентами. Это позволит превратить Соединенное Королевство в самую защищенную и привлекательную для жизни, бизнеса и инвестиций страну с цифровой экономикой.

5. Согласно нашему видению, **Соединенное Королевство в 2030 году по-прежнему будет ведущей ответственной и демократической кибердержавой, способной защищать и продвигать свои интересы в киберпространстве и с его помощью в поддержку достижения национальных целей. Это будет**:

- более защищенная и устойчивая страна, лучше подготовленная к эволюционирующим угрозам и рискам, которая использует свои кибер-возможности для защиты граждан от преступлений, мошенничества и угроз со стороны других государств;
- страна с инновационной процветающей цифровой экономикой, с более равномерным распределением возможностей в масштабах всей страны и всего многообразного населения;
- научно-техническая сверхдержава, обеспечивающая безопасное использование всего потенциала преобразующих технологий в интересах построения более экологически стабильного и здорового общества;
- более влиятельный и ценный партнер на мировой сцене, содействующий формированию будущих границ открытого и стабильного международного порядка при сохранении нашей свободы действий в киберпространстве.

6. За последнее десятилетие мы укрепили репутацию Соединенного Королевства как кибердержавы, наращивая передовой потенциал и оперативные возможности в области кибербезопасности и создавая ведущий сектор кибербезопасности. Настоящая стратегия опирается на значительный прогресс, достигнутый в ходе реализации Национальной стратегии кибербезопасности 2016–2021 года, и на три важных вывода, изложенных в Интегрированном обзоре политики в области безопасности, обороны, развития и иностранных дел. Во-первых, в цифровую эпоху кибермощь Соединенного Королевства становится еще более важным инструментом для достижения наших национальных целей. Во-вторых, для сохранения нашей кибермощи требуется более всеобъемлющая и комплексная стратегия, учитывающая весь спектр целей и возможностей в киберпространстве. И, в-третьих, нам требуется подход, предусматривающий участие всего общества: то, что происходит в зале заседаний или в классной комнате, имеет такое же значение для нашей национальной кибермощи, что и действия технических экспертов и правительственных чиновников, и работа в партнерстве является залогом нашего успеха.


CHELTENHAM
Science
Festival
18.2 Cyber Skills a
@CyNam

Пять основополагающих целей нашей стратегии

7. В Интегрированном обзоре изложены пять «первоочередных действий» в контексте настоящей стратегии, и мы используем их в качестве основополагающих целей нашего стратегического плана, **которые определяют направление и организацию конкретных действий, которые мы предпримем, и результатов, которых мы намереваемся достичь к 2025 году.**:

- **Основополагающая цель 1: укрепление кибернетической экосистемы Соединенного Королевства**, инвестиции в людей и подготовку квалифицированных кадров и углубление партнерских отношений между правительством, научными кругами и отраслью
- **Основополагающая цель 2: построение в Соединенном Королевстве устойчивой и процветающей цифровой экономики**, снижение киберрисков, позволяющее компаниям получать максимальные экономические выгоды от использования цифровых технологий, повышать безопасность граждан в интернете и укреплять их уверенность в том, что их данные надежно защищены
- **Основополагающая цель 3: достижение лидерства в области технологий, жизненно важных для кибердержавы,** наращивание промышленного потенциала и разработка механизмов, обеспечивающих доступ к будущим технологиям
- **Основополагающая цель 4: укрепление мирового лидерства и влияния Соединенного Королевства в целях формирования более надежного, благополучного и открытого международного порядка**, сотрудничество с правительственными и отраслевыми партнерами и обмен опытом и знаниями, на которые опирается кибермощь Соединенного Королевства
- **Основополагающая цель 5: обнаружение, дезорганизация и сдерживание наших противников в целях укрепления безопасности Соединенного Королевства в киберпространстве и с его помощью**, более комплексное, креативное и рутинное использование всего спектра рычагов, имеющихся в распоряжении Соединенного Королевства

8. В 1-й части этого документа описывается стратегический контекст нашей деятельности, цели нашей стратегии и стратегический подход, который мы примем в грядущем десятилетии. Во 2-й части описаны конкретные действия, которые мы предпримем для достижения наших целей к 2025 году, организованные согласно этим пяти основополагающим целям.

Видение

Согласно нашему видению, Соединенное Королевство в 2030 году по-прежнему будет ведущей ответственной и демократической кибердержавой, способной защищать и продвигать свои интересы в киберпространстве и с его помощью в поддержку достижения национальных целей.

Основополагающие цели и задачи

Основополагающая цель 1

Укрепление кибернетической экосистемы Соединенного Королевства

1. Укреплять структуры, партнерства и сети, необходимые для поддержки подхода к кибербезопасности, основанного на усилиях всего общества.
2. Укреплять и расширять кадровую базу квалифицированных киберспециалистов на всех уровнях, в том числе путем повышения престижа разносторонней профессии киберспециалиста мирового класса, которая вдохновляет и привлекает будущие перспективные кадры.
3. Активизировать рост устойчивого, инновационного и конкурентоспособного на международном уровне сектора информационной и кибербезопасности, поставляющего качественные продукты и услуги в соответствии с потребностями государства и экономики в целом

Основополагающая цель 2

Построение в Соединенном Королевстве устойчивой и процветающей цифровой экономики

1. Улучшить понимание киберрисков, чтобы повысить эффективность мер кибербезопасности и киберустойчивости.
2. Повысить эффективность предотвращения и сдерживания кибератак путем оптимизации управления киберрисками в британских организациях и улучшения защиты граждан.
3. Повышать устойчивость на национальном и организационном уровнях, чтобы быть готовыми к реагированию на кибератаки и восстановлению после них.

Основополагающая цель 3

Лидерство в области технологий, имеющих критическое значение для кибермощи

1. Повысить нашу способность предвосхищать, оценивать и использовать достижения науки и техники, имеющие жизненно важное значение для нашей кибермощи.
2. Наращивать и сохранять суверенные и союзнические преимущества в области безопасности технологий, имеющих критическое значение для киберпространства.

2a. Сохранять эффективность и устойчивость национального центра Crypt-Key, обеспечивающего удовлетворение потребностей государственных заказчиков, наших партнеров и союзников и принятие должных мер для снижения самых серьезных рисков, включая угрозы со стороны наиболее способных противников

3. Получить новейшее поколение подключаемых технологий и инфраструктуры, снижая риски для кибербезопасности, связанные с зависимостью от мировых рынков, и обеспечивая доступ британских пользователей к надежным и разнообразным источникам поставок.
4. Объединять усилия с многосторонними организациями для разработки мировых технических стандартов цифровых технологий в приоритетных областях, имеющих первостепенное значение для утверждения демократических ценностей, обеспечения кибербезопасности и укрепления британского стратегического преимущества с помощью достижений науки и техники.

Основополагающая цель 4

Укрепление глобального лидерства и влияния Соединенного Королевства

1. Укреплять кибербезопасность и устойчивость международных партнеров и расширять коллективную деятельность, направленную на дестабилизацию и сдерживание противников.
2. Формировать глобальную систему управления в интересах продвижения свободного, открытого и безопасного киберпространства.
3. Использовать и экспортировать британские средства и знания в области кибербезопасности в целях укрепления нашего стратегического преимущества и продвижения интересов в области внешней политики и процветания в общем.

Основополагающая цель 5

Обнаружение, сдерживание противников и противодействие им

1. Предпринимать меры для выявления государственных, криминальных и других субъектов киберпреступлений, расследования их вредоносной деятельности и обмена информацией о них в целях защиты Соединенного Королевства, его интересов и граждан.
2. Предпринимать меры для сдерживания государственных, криминальных и других субъектов киберпреступлений и противодействия их вредоносной деятельности, направленной против Соединенного Королевства, его интересов и граждан.
3. Предпринимать действия в киберпространстве и с его помощью в интересах национальной безопасности, а также предупреждения и выявления серьезных преступлений.

Содействие достижению национальных целей

- Безопасность и устойчивость
- Научно-техническая супердержава
- Экономическое процветание
- Формирование международного порядка

Часть 1.
Стратегия

Стратегический контекст

Глобальная Британия в эпоху соперничества

9. Интегрированный обзор политики в области безопасности, обороны, развития и иностранных дел, опубликованный в марте 2021 года, представляет, как правительство видит роль, которую Соединенное Королевство будет играть в мире в течение следующего десятилетия и действия, которые мы предпримем к 2025 году. В нем признается, что для того, чтобы Соединенное Королевство было лучше оснащено для успеха в более конкурентном мире, мы должны поощрять и использовать инновации в науке и технике в интересах повышения национального благосостояния и получения стратегического преимущества. Национальная киберстратегия опирается на этот подход и опубликована в соответствии с одним из обязательств, отраженных в Интегрированном обзоре, — «сохранение стратегического преимущества за счет использования достижений науки и техники».

Расклад сил в киберпространстве

10. Политические вызовы, которые создает киберпространство, не являются исключительно технологическими по своей природе. Кибер-домен — созданная человеком среда, которая формируется, в основном, под влиянием поведения человека. Она усиливает такое поведение будь то к лучшему или худшему, и последствия этого обычно ощущаются также в физическом мире. Киберпространством владеют и управляют частные компании, правительства, некоммерческие организации, отдельные граждане и даже преступники. Это означает, что при организации стратегического реагирования на этот контекст необходимо увязывать геостратегию с национальной безопасностью, уголовное правосудие с гражданским регулированием, экономическую политику с промышленной политикой, а также требуется глубокое понимание различного культурного или социального контекста и систем ценностей, взаимодействующих в интернете.

11. Киберпространство также не знает национальных границ. Технологические цепочки поставок и критические факторы зависимости приобретают все более глобальный характер, киберпреступники и государственные субъекты действуют из разных точек мира, влиятельные технологические компании экспортируют продукты и задают свои стандарты, и решения о правилах и нормах регулирования киберпространства и интернета принимаются на международных форумах. С развитием технологий и изменением способов их использования людьми киберпространство также постоянно эволюционирует, и это требует от нас принятия гибкого и оперативного подхода.

Уровни киберпространства

Что такое киберпространство?

Для многих из нас киберпространство является виртуальным миром, опыт взаимодействия с которым мы получаем, когда выходим в интернет, чтобы общаться, работать и выполнять повседневные задачи. В техническом понимании киберпространство — это взаимосвязанная и взаимозависимая сеть информационных технологий, включая интернет, телекоммуникационные сети, компьютерные системы и подключенные к интернету устройства. С военной точки зрения и в контексте усилий, направленных на противодействие угрозам в киберпространстве, оно рассматривается как один из операционных доменов, наряду с морским, сухопутным, воздушным и космическим доменами.

Как используется киберпространство? Киберпространство по определению является пространством «общего пользования», и, учитывая его масштабы и сложность, опыт его использования является уникальным для каждого отдельного человека. Люди получают доступ к киберпространству, когда проверяют свои банковские счета или смотрят дома кинофильмы в потоковом режиме. Компании используют киберпространство, чтобы предоставить персоналу доступ к необходимым ресурсам, будь то информация или средства управления производственным процессом. Правительства предоставляют своим гражданам государственные услуги через интернет-порталы. Кибер-специалисты заглядывают «под капот» технологий, стандартов и протоколов, обеспечивая, чтобы все хорошо работало и у пользователей не было проблем. Все эти группы используют киберпространство по-разному и в разных целях, и мы все находим ему всё более широкое применение.

Пользование интернетом

- Учетные записи электронной почты
- Учетные записи на игровых платформах
- Учетные записи в социальных сетях
- Данные для доступа к банковским счетам
- Бесконтактное проездное удостоверение
- Учетные записи для фитнес-браслетов

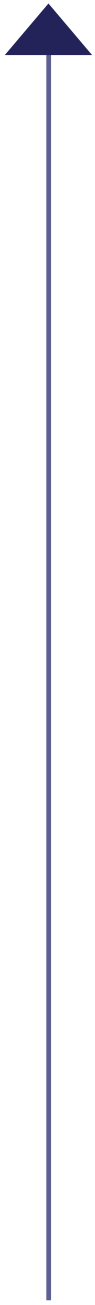
ПО, системы и данные

- Корпоративные ИТ-системы
- Базы данных, например, налоговые документы Британского управления по налогам и таможенным сборам
- Промышленные системы управления
- Операционные системы Windows/OS
- Приложения, например, WhatsApp, Facebook, TikTok
- Языки программирования, Python, C++

Физические устройства и связь

- Маршрутизаторы, концентраторы
- Серверы
- WiFi, Ethernet
- Радиоантенны
- Умные холодильники
- Считыватель бесконтактных проездных карт
- Телефоны, персональные компьютеры и другие персональные устройства

Киберпространство можно описать в контексте трех уровней:



ПОЛЬЗОВАНИЕ КИБЕРПРОСТРАНСТВОМ

Виртуальный

Эта та часть киберпространства, которой пользуются большинство людей. Она состоит из саморепрезентаций людей и организаций в общем виртуальном пространстве с помощью виртуальных личностей. Виртуальная саморепрезентация может быть в виде адреса электронной почты, идентичности пользователя, учетной записи в социальной сети или псевдонима. Один человек или одна организация может иметь множество личностей в интернете. И наоборот, множество людей или организаций также могут создать одну общую личность.

Логический

Эта часть киберпространства состоит из кода или данных, например, операционные системы, протоколы, приложения и другие программы. Логический уровень не может функционировать без физического уровня и передачи информации по проводным сетям или с помощью электромагнитных волн. Логический и физический уровни обеспечивают возможности для связи между виртуальными личностями и их деятельности.

Физический

Физический уровень киберпространства включает в себя все оборудование, используемое для передачи данных, начиная с маршрутизаторов, проводов и концентраторов в ваших домах и заканчивая крупными комплексными телекоммуникационными системами, эксплуатируемыми крупными технологическими компаниями. Помимо физической инфраструктуры, он также включает спектр электромагнитных волн, используемый для передачи данных, например беспроводные сети или радиосвязь.

Кибермощь

12. В основе нашей стратегии лежит концепция кибермощи, которую мы определяем как способность государства защищать и продвигать свои национальные интересы в киберпространстве и с его помощью. Мы определили пять широких аспектов кибермощи, которые согласуются с основополагающими целями этой стратегии:

- люди, знания, навыки, структуры и партнерства, которые являются основой нашей кибермощи, поддерживающей все другие компоненты и интегрирующей их в рамках национального подхода;
- способность защищать наши активы путем укрепления кибербезопасности и устойчивости в интересах реализации всех преимуществ, которые киберпространство обеспечивает для наших граждан и экономики;
- технические и промышленные возможности, обеспечивающие сохранение наших позиций в развитии ключевых кибертехнологий и применении новых достижений в интересах общества;
- глобальное влияние, взаимоотношения и этические стандарты, способствующие формированию правил и норм поведения в киберпространстве в соответствии с нашими ценностями и интересами и укреплению международной безопасности и стабильности;
- способность предпринимать действия в киберпространстве и с его помощью в интересах национальной безопасности, экономического благополучия и предупреждения преступности. Сюда входят кибероперации, способствующие получению результатов в реальном мире и достижению стратегического преимущества, а также операции правоохранительных органов и применение киберсанкций в целях привлечения к ответственности киберпреступников и подрыва их деятельности.

13. Кибермощь стоит отдельно от более традиционных форм силы. Она требует органичного сочетания потенциала жесткой силы с более мягкими рычагами влияния. Она имеет более распределенный характер, и правительства должны объединять усилия с партнерами, чтобы наращивать и использовать ее. И на фоне стремительного технологического прогресса ее можно так же быстро получить, как и утратить, так как возможности, ранее бывшие передовыми, устаревают с появлением новых достижений.

14. Это отражено в нашей стратегии, описывающей, как мы будем работать вместе с партнерами везде, где это возможно, в рамках усилий всего общества. Мы будем прилагать больше усилий к тому, чтобы решать проблемы у их истоков и устранять коренные причины, предвосхищать будущие тенденции и принимать долгосрочные меры реагирования, а также будем более активно участвовать в формировании конкурентной геополитической среды, а не просто реагировать на ее эволюцию.

Соединенное Королевство как кибердержава сегодня

15. Соединенное Королевство уже является ведущей кибердержавой.[1] В минувшее десятилетие наше правительство возглавляло настойчивые национальные усилия, направленные на укрепление кибербезопасности Соединенного Королевства, повышение осведомленности общественности о киберрисках, развитие сектора кибербезопасности и наращивание широкого спектра возможностей для реагирования на угрозы со стороны враждебных субъектов с помощью киберпространства. Хотя мы достигли значительного прогресса и заняли сильные позиции, перед нами все еще стоят серьезные вызовы в области всех пяти основополагающих целей этой стратегии.

[1] Занимает второе место в Глобальном индексе кибербезопасности по версии Совета Международного союза электросвязи, третье — в Индексе кибермощи по версии Центра имени Белферов при Гарвардском университете, и входит во вторую группу согласно оценке кибермощи, выполненной Международным институтом стратегических исследований.

Кибернетическая экосистема и технологическое лидерство Соединенного Королевства

16. Подход Соединенного Королевства к наращиванию кибермощи включает в себя согласованные усилия по развитию кадровой базы киберспециалистов и коммерческого потенциала, при этом правительство Соединенного Королевства и автономные правительства Северной Ирландии, Шотландии и Уэльса работают в партнерстве друг с другом, обмениваясь опытом и знаниями. Британский сектор кибербезопасности быстро растет и насчитывает более 1400 компаний, совокупный доход которых в прошлом году составил 8,9 млрд фунтов стерлингов. Сектор обеспечивает 46 700 квалифицированных рабочих мест и привлекает крупные иностранные инвестиции. Этот сектор имеет жизненно важное значение для укрепления нашей кибермощи, обеспечивая повышение безопасности, укрепление международного влияния и стимулирование экономического роста. Мы укрепляем репутацию Соединенного Королевства как мирового лидера в области исследований кибербезопасности, имея 19 центров передового академического опыта и 4 исследовательских института, занимающихся наиболее актуальными проблемами кибербезопасности.

17. Число работников, занятых в секторе кибербезопасности, увеличилось почти на 50% за последние четыре года, причем спрос на квалифицированных работников зачастую превышает предложение. Мы активно взаимодействуем с отраслевыми предприятиями, профессиональными организациями, студентами, работодателями, имеющимися специалистами по кибербезопасности и образовательными учреждениями, чтобы лучше понять природу вызова, связанного с удовлетворением потребностей в квалифицированных киберспециалистах. Мы реализовали широкий спектр внепрограммных инициатив, чтобы вызвать у молодых людей интерес к карьере в области кибербезопасности. В период с 2019 по 2020 год мы привлеки около 57 тысяч молодых людей к участию в наших учебных программах CyberFirst и Cyber Discovery. Мы расширили рамки наших курсов, чтобы охватить более молодых учащихся. Так, в интернет-конкурсе CyberFirst Girls приняли участие 11 900 девочек, при этом соревнования ведущих команд проводились одновременно в 18 центрах по всему Соединенному Королевству. Программа предоставления стипендий CyberFirst позволила привлечь целеустремленных и талантливых студентов. В прошлом году в программе принимали участие 750 человек, и все 56 выпускников получили постоянную работу в сфере кибербезопасности.

18. Несмотря на эти меры, формирование квалифицированного кадрового резерва все еще представляет собой серьезный вызов: примерно половина из 1,32 млн компаний в разных секторах экономики сообщают о нехватке базовых технических специалистов по кибербезопасности.[2] И хотя британский сектор кибербезопасности стремительно растет, большинство компаний являются стартапами, и масштабное наращивание базы национальных поставщиков остается сложной задачей в условиях растущей международной консолидации. И, как показал опыт с 5G, Соединенное Королевство и его союзники не занимают лидирующие позиции в некоторых ключевых областях индустрии технологий в целом. Страны, способные играть лидирующую роль в сфере технологий, критически важных для наращивания кибермощи, будут иметь больше возможностей, чтобы влиять на пути и методы их разработки и развертывания, и смогут лучше защищать свою безопасность, обеспечивать экономическое преимущество и оперативнее использовать возможности для совершения прорывов в разработке киберсредств.

Киберустойчивость Соединенного Королевства

19. В последнее десятилетие нами принят широкий диапазон мер, направленных на укрепление киберустойчивости Соединенного Королевства. Это стало возможно благодаря крупным и долгосрочным инвестициям в некоторые из наших ключевых кибер-возможностей, в том числе в Национальный центр кибербезопасности (NCSC), правоохранительные органы и в специалистов по безопасности и политике в масштабах всего правительства, а также в расширение национальных и международных партнерств.

[2] DCMS, Cyber security skills in the UK labour market 2021 (2021)

20. Наши самые инновационные и прорывные усилия были сосредоточены на широкомасштабных действиях, в том числе в рамках разработки и расширения масштабов развертывания программы «Активная киберзащита» (ACD). В прошлом году в ходе ее осуществления было нейтрализовано 2,3 млн вредоносных кампаний, в том числе 442 фишинговые кампании, проводившиеся с использованием бренда NHS, и 80 фальшивых приложений NHS, размещенных и доступных для загрузки в неофициальных магазинах приложений.[3] Мы также первыми в мире выступили за то, чтобы подключаемые к интернету потребительские продукты были «безопасными по дизайну», разработав в 2018 году Кодекс практики, который вдохновил других последовать нашему примеру и лег в основу первого общемирового отраслевого стандарта для подключаемых к интернету потребительских устройств.[4] [5]

21. Новый регламент имел положительный эффект на кибербезопасность: 82% организаций отмечали, что улучшения, которых им удалось добиться, были результатом введения в действие Общего регламента по защите данных Соединенного Королевства в 2018 году.[6] И 77% компаний сегодня считают кибербезопасность одним из своих главных приоритетов, что на 12% больше, чем 2016 году.[7] Введение в действие Положений о сетях и информационных системах («Положения NIS») в 2018 году также привело к тому, что назначенные организации приняли меры по повышению безопасности своих сетей и информационных систем, что привело к снижению киберрисков для жизненно важных услуг и цифровых сервисов особого значения.[8] Хорошим примером сотрудничества в масштабе четырех наций в составе Соединенного Королевства стало обеспечение улучшений в секторе здравоохранения, в том числе выполнение требований Положений NIS.

22. Мы предоставили организациям, работающим в разных секторах экономики, всеобъемлющие консультации и инструкции по кибербезопасности, а также оказали адресную поддержку предприятиям в критически важных секторах в период пандемии коронавируса (COVID-19). В рамках кампании Cyber Aware мы предоставили населению рекомендации о мерах, которые можно предпринять, чтобы защитить себя в интернете. В случае успешных кибератак мы задействовали наши передовые возможности реагирования на инциденты, предоставляя прямую поддержку в самых серьезных случаях, а благодаря инвестициям в подготовку специалистов местных правоохранительных органов мы теперь реагируем на все инциденты, о которых поступают сообщения.

23. Мы образовали специализированные подразделения кибербезопасности в правоохранительных органах в масштабах всего Соединенного Королевства, которые действуют наряду с сетью PROTECT, Подразделением по работе с жертвами экономических преступлений и региональными Центрами киберустойчивости. Благодаря этим инициативам наши граждане, а также и малые и средние предприятия, всегда могут обратиться за поддержкой и рекомендациями по повышению киберустойчивости к обладающим необходимыми навыками и местными знаниями специалистам, которые находятся неподалеку или доступны для связи.

24. Тем не менее, у нас есть все больше данных, свидетельствующих о пробелах в нашей системе национальной устойчивости: продолжает расти киберпреступность и учащаются случаи

---

[3] NCSC, NCSC Annual Review 2021 (2021)
[4] Министерство цифровизации, культуры, СМИ и спорта, Code of Practice for Consumer IoT Security (2018)
[5] Министерство цифровизации, культуры, СМИ и спорта, ETSI industry standard based on the Code of Practice (2019)
[6] Министерство цифровизации, культуры, СМИ и спорта/RSM, The impact of GDPR on cyber security outcomes (2020). Общий регламент по защите данных (GDPR) был принят в 2018 году, в настоящее время его заменил Общий регламента по защите данных Соединенного Королевства (UK GDPR).
[7] Министерство цифровизации, культуры, СМИ и спорта, Cyber Security Breaches Survey 2021 (2021)
[8] Министерство цифровизации, культуры, СМИ и спорта, Post-Implementation Review of the Network and Information Systems Regulations 2018 (2020)

нарушения безопасности, затрагивающие правительства, компании и граждан, и кибер-активированных преступлений, таких как мошенничество.[9] [10] Унаследованные ИТ-системы, уязвимости цепочек поставок и нехватка специалистов по кибербезопасности — области, вызывающие растущую обеспокоенность. Почти четыре из десяти компаний (39%) и четвертая часть благотворительных организаций (26%) сообщают, что в минувшем году они пострадали от нарушений системы кибербезопасности или кибератак, и многие организации (особенно малые и средние предприятия) не способны защитить себя и реагировать на инциденты.[11] Согласно отраслевым данным, многие компании не понимают стоящих перед ними киберрисков, у них отсутствует четкое понимание коммерческих выгод инвестирования в кибербезопасность и мотивация для сообщения о нарушениях и атаках.

Лидерство и влияние Соединенного Королевства на мировой арене

25. На международном уровне британский опыт и знания в области кибертехнологий получают высокую оценку со стороны наших партнеров, и Соединенное Королевство играет определяющую роль в укреплении международного потенциала и решимости противостоять вредоносной кибердеятельности. Это подкрепляется ответственным использованием наших наступательных кибер-возможностей в соответствии с британским и международным законодательством и нашими публично изложенными позициями — в отличие от нерегулируемой деятельности некоторых наших противников.

26. В период своего председательства в Содружестве Наций Соединенное Королевство инициировало и возглавило осуществление Декларации Британского Содружества наций о деятельности в киберпространстве, подтвердившей наши общие обязательства в области безопасности, процветания и ценностей в киберпространстве. В рамках международной сети своих контактов Национальное агентство по борьбе с преступностью (NCA) укрепляет партнерские связи с зарубежными правоохранительными органами в области кибербезопасности, опираясь на отношения, сложившиеся в течение долгой истории совместного оперативного реагирования на угрозы. Соединенное Королевство также увеличило свою сеть специалистов по кибер- и технологической безопасности за рубежом на пяти континентах и предприняло усилия по наращиванию потенциала в 100 странах, повышая их устойчивость, укрепляя британское влияние и продвигая ценности Соединенного Королевства.

27. В рамках Программы Специальных представителей по кибербезопасности мы наладили долгосрочные отношения на международном уровне и помогли британским компаниям получить крупные международные контракты. В рамках британских инициатив в области международного развития, таких как Программа цифрового доступа, осуществляется успешное сотрудничество с партнерскими странами в Африке, Азии и Латинской Америке. Мы предоставляем им техническую помощь в укреплении потенциала кибербезопасности их государств, бизнес-секторов и пользователей в том числе путем улучшения навыков кибергигиены в сообществах, обслуживаемых в недостаточной степени, чтобы дать возможность наиболее уязвимым людям защитить себя от рисков и вызовов, связанных с присутствием в интернете.

28. Однако на международном уровне мы сталкиваемся с конкурирующими подходами, поскольку системные противники, такие как Китай и Россия, продолжают настаивать на том, что ответом на вызовы безопасности является расширение национального суверенитета над киберпространством. Свобода интернета в мире ограничивается, и существует риск того, что видение интернета как совместно используемого пространства в интересах содействия обмену знаниями и товарами между открытыми обществами, окажется под угрозой.

---

[9] Квалифицируются как правонарушения, предусмотренные Законом о неправомерном использовании компьютерных технологий

[10] Национальная статистическая служба, Crime in England and Wales: year ending June 2021 (2021)

[11] Министерство цифровизации, культуры, СМИ и спорта, Cyber Security Breaches Survey 2021 (2021)

Противодействие киберугрозам для Соединенного Королевства и сдерживание наших противников

29. Угрозы, которые стоят перед нами в киберпространстве и в связи с его использованием, в последнее время становятся все более интенсивными, сложными и серьезными. Соединенное Королевство подвергается кибератакам со стороны растущего круга государственных субъектов, криминальных групп (иногда действующих по указанию государств или с их косвенного одобрения) и активистов, преследующих цели шпионажа, коммерческой выгоды, саботажа и дезинформации. Такие атаки приводят к серьезным финансовым потерям, краже интеллектуальной собственности, психологическому стрессу, перебоям в предоставлении услуг и работе активов, а также к возникновению рисков для нашей критической национальной инфраструктуры, демократических институтов и средств распространения информации. Они также могут подорвать доверие инвесторов и потребителей и усугубить существующее неравенство и уже причиненный ущерб. В период пандемии COVID-19 онлайновые атаки способствовали дальнейшему усугублению теневой пандемии гендерного насилия. Атаки программ-вымогателей становятся все более изощренными и вредоносными. Тогда как общий уровень киберугроз со стороны враждебных субъектов во время пандемии COVID-19 не изменился, злоумышленники воспользовались открывающимися возможностями, чтобы переориентировать свои кибероперации на кражу данных о разработке вакцин и результатов медицинских исследований, а также на ослабление других наций, уже пострадавших от кризиса. Подверженность рискам также возрастает ввиду растущей зависимости удаленной работы и интернет-транзакций от цифровых технологий. Наряду с этим, цифровой разрыв также обусловливает неравный доступ к интернет-услугам и подвергает людей угрозе надругательства и причинения вреда в интернете ввиду недостаточной цифровой грамотности и осведомленности о мерах кибербезопасности, которые мы все можем предпринять, чтобы защитить себя в интернете.[12]

30. Правительство предпринимает меры для противодействия этим растущим угрозам. Значительные инвестиции в разведывательный потенциал позволили углубить понимание этих угроз и проводить более эффективные секретные кампании по противодействию им. Мы разработали комплекс правоохранительных мер реагирования на киберпреступления, осуществляемые под руководством Национального агентства по борьбе с преступностью (NCA), и образовали специальные группы кибербезопасности в составе региональных подразделений по борьбе с организованной преступностью и местной полиции в Англии, Уэльсе, Северной Ирландии и Шотландии. Это укрепило наше операционное и разведывательное преимущество над киберпреступниками и другими противниками. Правительство также разрабатывает британскую структуру доверия для проверки идентичности и других атрибутов, которая повысит безопасность растущего числа решений для цифровой идентификации.[13] Это также будет содействовать борьбе с преступлениями, связанными с неправомерным использованием идентификационных данных. Программа NCA «Cyber Choices» помогает людям делать более обоснованный выбор, отвращая их от преступной деятельности и поощряя их к использованию своих кибернавыков позитивным и законным образом.

31. Мы вложили значительные средства в наступательный киберпотенциал, сначала в рамках Национальной программы наступательных кибероперации, и в последнее время — в рамках образования Национальных сил кибербезопасности (NCF). В составе NCF впервые под единым командованием был объединен персонал Центра правительственной связи (GCHQ), Министерства обороны (МО), Секретной разведывательной службы (SIS, также известной как MI6) и Лаборатории оборонной науки и техники. Эти силы осуществляют операции в киберпространстве и при его помощи в целях обеспечения безопасности страны, а также защиты и продвижения интересов Соединенного Королевства внутри страны и за ее пределами.

[12] NCSC, CyberAware

[13] Министерство цифровизации, культуры, СМИ и спорта UK digital identity and attributes trust framework (2021)

32. В сотрудничестве с союзниками мы также стремимся добиваться того, чтобы спонсируемая государствами враждебная деятельность в киберпространстве оборачивалась для них большими потерями, путем присвоения ответственности — как мы недавно сделали в случае нарушений SolarWinds и Microsoft Exchange — и принятия мер для наступления последствий для тех, кто несет за эти действия ответственность. Разработка автономного британского режима киберсанкций добавила еще один разрушительный инструмент в арсенал средств, которые мы используем для реагирования на такие инциденты, как атаки с использованием вирусов WannaCry и NotPetya. Однако, несмотря на все эти меры, наш подход к сдерживанию кибератак, по видимости, пока еще не привел к фундаментальным изменениям в калькуляции рисков для нападающих. Далее описываются некоторые недавние примеры серьезных кибератак.

Примеры недавних случаев кибератак

В течение 2021 года Соединенное Королевство совместно с международными партнерами продолжило работать над обнаружением и ликвидацией общих угроз, большинство из которых стабильно исходит от России и Китая. Стало очевидно, что в дополнение к прямым киберугрозам, создаваемым Российским государством, в России находятся многие организованные преступные группировки, совершающие атаки с использованием программ-вымогателей против западных объектов. Китай, с его растущими амбициями по проецированию влияния на территории за пределами его границ и хорошо известным интересом к британским коммерческим тайнам, продолжает оставаться высокотехнологичным субъектом деятельности в киберпространстве. То, как Китай будет развиваться в течение следующего десятилетия будет, вероятно, самым серьезным из отдельных факторов, определяющих будущее кибербезопасности Соединенного Королевства. Вместе с тем, менее технологичные, чем Россия и Китай, Иран и Северная Корея продолжают использовать средства цифрового вторжения для достижения своих целей, в том числе путем кражи и саботажа.

Киберпреступники используют программы-вымогатели для атак на государственные службы

Программы-вымогатели стали самой значительной из киберугроз, с которыми Соединенное Королевство столкнулось в 2021 году. Учитывая возможные серьезные последствия успешной атаки на жизненно важные услуги и критическую национальную инфраструктуру, NCSC считает программы-вымогатели потенциально такими же вредоносными, как и спонсируемый государством шпионаж.[14]

В октябре 2020 года местный совет Хакни подвергся атаке программы-вымогателя, которая привела к многомесячным перебоям в его работе и потребовала миллионы фунтов стерлингов для восстановления. В критически важное время, когда совет занимался преодолением последствий пандемии COVID-19, он был лишен доступа к важным данным и была нарушена работа многих служб, в том числе сбор муниципального налога и выплата пособий. Подобным атакам подверглись другие местные органы власти, а также ряд организаций в сфере образования.

[14] NCSC, Mitigating malware and ransomware attacks (2021)

В мае 2021 года в результате атаки программы-вымогателя на Службу здравоохранения Ирландии (HSE) на 10 дней была парализована работа ИТ-сетей и больниц в структуре здравоохранения Ирландии, что имело реальные последствия для пациентов и их семей. Похищенные данные некоторых пациентов также были опубликованы в интернете. Служба HSE, которая занимается оказанием услуг здравоохранения и социального обслуживания в Ирландии, отключила национальную и региональные сети в тот же день, чтобы не допустить эскалации инцидента. Признаки вредоносной кибердеятельности также были обнаружены в сети Департамента здравоохранения Ирландии (DoH), однако в результате развертывания инструментов в процессе расследования попытка запустить программу-вымогателя была обнаружена и пресечена. Эта атака также затронула Северную Ирландию, нарушив доступ некоторых трансграничных медицинских служб к данным пациентов, хранящимся в HSE.

Важно отметить, что ни в одном из этих случаев выкуп выплачен не был. **Правоохранительные органы не поощряют, не одобряют и не оправдывают уплаты выкупа. Если вы платите выкуп:**

- **нет никаких гарантий, что вы получите доступ к своим данным или компьютеру;**
- **ваш компьютер будет все еще заражен вредоносной программой;**
- **вы отдадите свои деньги криминальным группировкам;**
- **вы с большей вероятностью будете объектом для нападения в будущем.**

NCSC опубликовал рекомендации для организаций по защите от атак вредоносного ПО или программ-вымогателей, в том числе по подготовке к инцидентам и по мерам, которые организациям следует предпринять в случае заражения.

Государства, использующие стратегические уязвимости и цепочки поставок в своих интересах

Случаи с компрометацией провайдера программного обеспечения SolarWinds и использованием уязвимостей серверов Microsoft Exchange привлекли внимание к угрозе, связанной с атаками на цепочку поставок. Эти две изощренные атаки, объектом нападения которых стали менее защищенные элементы — такие как поставщики управляемых услуг или коммерческие программные платформы — в цепочке поставок экономических и правительственных организаций и национальных органов безопасности, были самыми серьезными кибервторжениями, известными NCSC.

В начале декабря 2020 года североамериканская компания FireEye, работающая в области кибербезопасности, обнаружила, что злоумышленнику удалось внедрить вредоносную модификацию в продукт, используемый этой компанией и многими другими организациями по всему миру. Эта модификация позволяла злоумышленнику запускать команды уровня администратора на любом устройстве, на котором установлен зараженный продукт, и могла быть использована для дальнейших целенаправленных атак на подключенные системы. Исходная атака на цепочку поставок была осуществлена через программу Orion, предназначенную для мониторинга ИТ-сетей, которая была разработана компанией **SolarWinds**. Злоумышленнику удалось внедрить вредоносный код в обновление для этой программы еще в марте 2020 года. В апреле 2021 года NCSC вместе со своими североамериканскими коллегами из органов безопасности впервые объявили о том, что за этой атакой — одной из самых серьезных за последнее время — стоит Служба внешней разведки (СВР) России.[15] Компания SolarWinds подтвердила, что в результате этой атаки пострадали 18 тысяч организаций по всему миру, включая правительственные учреждения США. Этот инцидент был одним из широкого ряда кибервторжений со стороны СВР, которая ранее предпринимала попытки получить доступ к ИТ-сетям стран-членов НАТО и европейских государств.

[15] МИДСР, Russia: UK and US expose global campaign of malign activity by Russian intelligence services (2021).

2 марта 2021 года компания Microsoft обнародовала информацию о том, что ряд серверов **Microsoft Exchange**, которые организации по всему миру используют для управления электронной почтой, планированием и совместной работой, подвергся атаке со стороны высокотехнологичного субъекта. Согласно оценке Microsoft, первые вторжения начались еще в январе 2021 года и спонсировались китайским государством. В ответ на атаку компания выпустила ряд обновлений безопасности для уязвимых серверов. В июле 2021 года Соединенное Королевство совместно с единомышленниками подтвердило, что ответственность за атаки, затронувшие более 250 тысяч серверов по всему миру, несут субъекты, действующие при поддержке китайского государства.[16] Эти атаки, по всей вероятности, преследовали создание возможностей для широкомасштабного шпионажа, включая получение доступа к идентифицирующей личность информации и интеллектуальной собственности. Компрометация серверов Microsoft Exchange дала злоумышленнику опору для дальнейшего внедрения в ИТ-системы жертв. Во время атаки правительство оперативно предоставило пострадавшим советы и рекомендации по необходимым мерам, и компания Microsoft заявила, что к концу марта 92% клиентов установили обновления для защиты от этой уязвимости.

[16] МИДСР, UK and allies hold Chinese state responsible for a pervasive pattern of hacking (2021)

Движущие силы перемен

33. В наступающем десятилетии мы станем свидетелями **дальнейшего стремительного расширения использования данных и цифровых каналов практически в каждом аспекте нашей жизни**. Взрывной рост доступа к интернету и масштабов его использования, опирающийся на данные и их инфраструктуру, приводит к созданию новых рынков, повышению удобства и эффективности и расширению возможностей выбора. Но это также значительно повышает зависимость стран от взаимосвязанных цифровых систем, открывая больше возможностей для вредоносной деятельности и существенного воздействия на «реальный мир». На фоне продолжающегося сближения критических и не критических технологий в масштабах многих секторов эти риски распространяются на новые области нашей экономики, и перенос данных и сервисов в облако — и зачастую за пределы Соединенного Королевства — еще более повышают уровень подверженности рискам.

34. Мы все чаще наблюдаем примеры взаимодействия между компаниями, давно и успешно работающими в регулируемых секторах, таких как телекоммуникации и энергетика, и новыми компаниями в преимущественно нерегулируемых секторах, которые, например, обеспечивают возможности в области микрогенерации, зарядки электромобилей или «умных городов». Критическая инфраструктура станет еще более распределенной и рассредоточенной, и это коренным образом изменяет то, как регулирование будет влиять на безопасность критических функций и сервисов, на которые мы полагаемся. Эта диверсификация также затронет национальную безопасность в целом, усложняя получение доступа к информации будь то для органов правопорядка или служб кибербезопасности. Это изменение среды также затронет продукты и услуги за пределами традиционной критической национальной инфраструктуры.

35. По мере **постоянного усложнения ландшафта** государствам, компаниям и обществу будет все труднее понимать, какие риски стоят перед ними и как они могут и должны защищать себя от угроз. Повышение зависимости от сторонних поставщиков управляемых услуг, которые часто имеют привилегированный доступ к ИТ-системам тысяч клиентов, создает новые риски, которыми необходимо управлять. Подключение устройств и сетей к iинтернету все чаще будет стандартной характеристикой, и киберпространство охватит наши дома, автомобили, урбанизированные среды и промышленную инфраструктуру. Сенсорные, носимые, медицинские и биометрические устройства еще больше стирают границы между деятельностью оффлайн и онлайн. Киберриски становятся всепроникающими, что приводит к увеличению объема генерируемых персональных и чувствительных данных и масштаба возможных последствий в случае нарушения безопасности систем.

36. На этом фоне **продолжится эволюционирование и диверсификация угроз в киберпространстве** по мере того, как высокотехнологичные кибер-возможности будут становиться общедоступными и распространяться среди широкого круга государств и криминальных группировок. Увеличится количество субъектов, имеющих возможности и намерение атаковать Соединенное Королевство в киберпространстве, и государства будут прибегать к более широкому спектру рычагов для ведения подрывной деятельности, в том числе через посредников. Ускорение перехода к гибридным методам работы и введение ограничений на международные поездки в связи с пандемией привели к увеличению зависимости от цифровых услуг и мотивировали организованные криминальные группировки на совершение киберпреступлений. Мы уже видим признаки этой тенденции, и по данным последнего обзора преступности, в период с 2019 по 2021 год значительно возросло число киберпреступлений.[17] Этот вызов не уникален для Соединенного Королевства и приводит к возникновению взаимной уязвимости для всех, кто использует киберпространство.

[17] Национальная статистическая служба, Crime in England and Wales: year ending June 2021 (2021)

37. Конкуренция в киберпространстве будет обостряться на фоне стремления государственных и негосударственных субъектов к получению стратегических преимуществ в киберпространстве и с его помощью. Кибероперации будут становиться все более важным инструментом проецирования власти на уровне ниже порога вооруженного конфликта и предконфликтных ситуаций. Кроме того, в будущих конфликтах в большей мере будут задействованы кибер-возможности. Чтобы Соединенное Королевство могло действовать эффективно, нам требуется повысить уровень киберустойчивости нашего оборонного потенциала. Для эффективного устранения угроз и обеспечения оборонной деятельности в целом необходимо, чтобы кибероперации были интегрированы с другими элементами вооруженных сил. Наша деятельность в космическом домене будет расширяться, как описано в Национальной космической стратегии, что сопряжено с возникновением новых областей риска, но вместе с тем позволит Соединенному Королевству находить новые пути применения своих кибер-возможностей для получения преимуществ.[18]

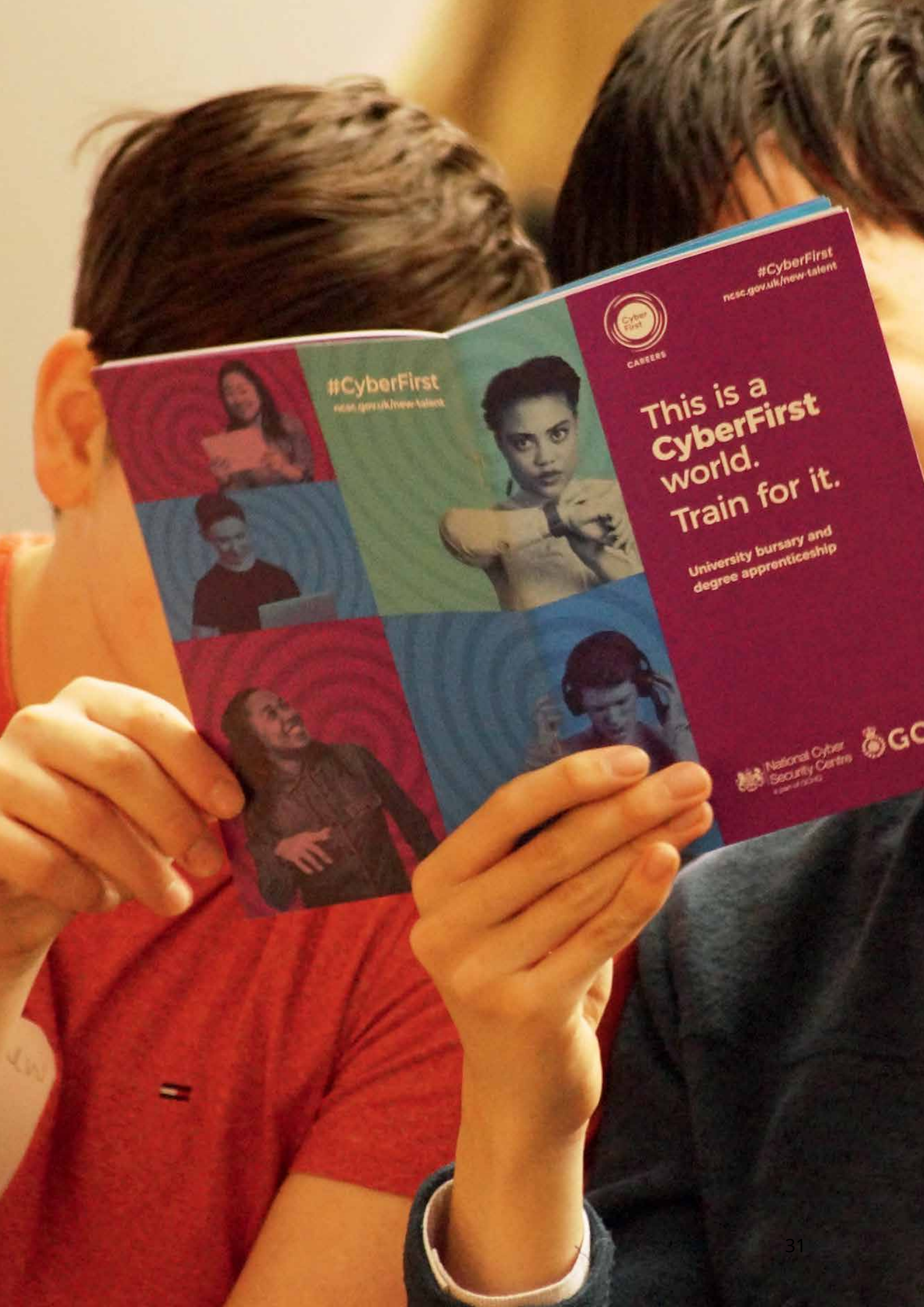
38. Дебаты о правилах, регулирующих киберпространство, все чаще будут становиться площадкой **системного противостояния между ведущими державами** на фоне столкновения ценностей стран, стремящихся сохранить основанную на открытом обществе систему, с одной стороны, и таких системных соперников, как Китай и Россия, настаивающих на усилении государственного контроля как единственного способа обеспечить безопасность киберпространства. Это будет оказывать давление на свободный и открытый интернет, в то время как национальные государства, крупные технологические компании и другие субъекты продвигают конкурирующие подходы к разработке технических стандартов и управлению интернетом.

39. Эту проблему усугубит **борьба за контроль над стремительно эволюционирующим технологическим ландшафтом**. С интеграцией цифровых технологий в нашу повседневную жизнь, деятельность компаний и инфраструктуру некоторые технологии приобретают поистине критическое значение для функционирования общества. Власть будет все более сосредоточиваться в руках стран, имеющих стратегическое преимущество в области науки и техники и доступ к данным, двигающим инновации, что позволит им оказывать влияние на других и формировать глобальные стандарты в соответствии со своими экономическими и политическими интересами.

40. Нарождающиеся технологии, такие как цифровые двойники, квантовые вычисления и широкомасштабные автономные системы — равно как и генерируемая ими информация — будут создавать новые возможности и риски, а также откроют доступ к новым кибер-возможностям для нападающих и обороняющихся, как например в случае использования вымогателями криптовалюты. Технологическое лидерство становится более рассредоточенным, и Соединенное Королевство не сможет наращивать суверенный потенциал в области всех технологий, которые имеют критическое значение. Государства и компании используют технические стандарты для продвижения своих интересов, и существует опасность того, что ключевые технологии будут формировать те, кто не разделяет наших ценностей.

41. Уже более десяти лет Соединенное Королевство осуществляет амбициозную национальную стратегию кибербезопасности и сохраняет высокий уровень инвестиций, укрепляя положение страны в качестве глобального лидера в киберпространстве. Как следует из представленного выше анализа, вызовы и возможности по-прежнему сохраняются на высоком уровне. В следующих разделах описываются национальные меры реагирования.

[18] Правительство Соединенного Королевства, Национальная космическая стратегия (2021)


#CyberFirst
ncsc.gov.uk/new-talent
CAREERS
This is a CyberFirst world. Train for it.
University bursary and degree apprenticeship
National Cyber Security Centre

Меры национального реагирования

42. В сложившейся стратегической обстановке Соединенному Королевству предстоит сделать выбор. Мы можем просто стараться идти в ногу с угрозами и вызовами, стоящими перед нами в киберпространстве, которое носит все более комплексный характер, консолидируя прогресс, достигнутый за последние пять лет, и по мере возможностей решая наиболее неотложные вопросы. Этот подход сопряжен с двумя рисками. Во-первых, мы не полностью реализуем потенциал сильной британской базы в сфере кибертехнологий для защиты национальных приоритетов и упустим возникающие возможности. Во-вторых, гораздо более серьезная опасность заключается в том, что мы достигнем точки невозврата в развитии технологии и обнаружим, что основы нашей будущей экономики и общества формируют наши конкуренты и противники, и что нам придется прилагать больше усилий для обеспечения своей безопасности.

43. Мы считаем, что с дальнейшим усилением основополагающей роли киберпространства в обеспечении наших интересов и интересов наших союзников и противников **укрепление нашего конкурентного преимущества при маневрировании в этой обстановке становится стратегической необходимостью**. Это позволит нам не только обеспечить свою безопасность сегодня, но и содействовать формированию завтрашнего мира и пользоваться его благами.

Наше видение, цели и принципы

44. Согласно нашему видению, Соединенное Королевство в 2030 году по-прежнему будет **ведущей ответственной и демократической кибердержавой, способной защищать и продвигать свои интересы в киберпространстве и с его помощью в соответствии с нашими национальными целями**.

45. Для претворения этого видения в жизнь мы будем стремиться к достижению пяти стратегических целей. По отдельности каждая из них направлена на укрепление нашего национального потенциала в одном из пяти измерений кибермощи, и вместе они призваны содействовать повышению нашей способности к утверждению принципов киберпространства, которые отражают наши ценности и интересы. Эти пять основополагающих целей формируют стратегическую рамочную программу, направляющую нашу деятельность. Во 2-й части описаны действия, которые мы будем предпринимать в период до 2025 года для достижения каждой цели.

- **Основополагающая цель 1: укрепление кибернетической экосистемы Соединенного Королевства**, инвестиции в людей и подготовку квалифицированных кадров и углубление партнерских отношений между правительством, научными кругами и отраслью
- **Основополагающая цель 2: построение в Соединенном Королевстве устойчивой и процветающей цифровой экономики**, снижение киберрисков, позволяющее компаниям получать максимальные экономические выгоды от использования цифровых технологий, повысить безопасность граждан в интернете и укрепить их уверенность в том, что их данные надежно защищены
- **Основополагающая цель 3: достижение лидерства в области технологий, жизненно важных для кибердержавы,** наращивание промышленного потенциала и разработка механизмов, обеспечивающих доступ к будущим технологиям
- **Основополагающая цель 4: укрепление мирового лидерства и влияния Соединенного Королевства в области создания более надежного, благополучного и открытого международного порядка**, сотрудничество с правительственными и отраслевыми партнерами и обмен опытом и знаниями, на которые опирается кибермощь Соединенного Королевства
- **Основополагающая цель 5: обнаружение, дезорганизация и сдерживание наших противников в целях укрепления безопасности Соединенного Королевства в киберпространстве и с его помощью**, более комплексное, креативное и рутинное использование всего спектра рычагов, имеющихся в распоряжении Соединенного Королевства

46. Эти цели призваны быть взаимоукрепляющими. Например, достижение более высоких уровней кибербезопасности и устойчивости на национальном уровне станет необходимой основой для более активной позиции на международном уровне. Далее, учитывая что наши цепочки поставок носят глобальный характер, а стоящие перед нами угрозы исходят из-за рубежа, мы не сможем обеспечить свою безопасность, если не будем более активно способствовать формированию поведения международных субъектов. Наша способность влиять на глобальные дебаты по вопросам киберпространства, интернета и технологий будет зависеть от сохранения технического преимущества и развития инновационной экосистемы, обеспечивающей получение реального преимущества в области технологий, которые имеют самое большое значение.

47. Центральное место в нашем видении занимает **продвижение свободного, открытого, мирного и безопасного киберпространства**. Наша стратегическая направленность на развитие кибермощи не означает стремления к разжиганию конфликта или к выигрышу Соединенного Королевства в игре с нулевой суммой. Как указано в Интегрированном обзоре, мир, в котором открытые общества и открытая экономика могут процветать, — лучшая гарантия нашего будущего благополучия, суверенитета и безопасности. Соединенное Королевство будет работать вместе со станами-единомышленниками над продвижением наших общих ценностей — открытости и демократии, — применяя **ответственный и демократический подход к наращиванию кибермощи**. Это означает, что в работе над достижением этих пяти стратегических целей мы будем руководствоваться следующими **принципами**:

- Одной из наших приоритетных задач будет обеспечение способности граждан и компаний безопасно пользоваться киберпространством, чтобы они могли получать максимальные экономические и социальные преимущества от цифровых технологий, а также пользоваться своими законными и демократическими правами

- Мы будем работать над утверждением открытого и функционально совместимого интернета как наилучшей модели для содействия глобальному процветанию и благополучию, а также противодействовать давлению со стороны авторитарных государств, отстаивающих фрагментацию и свою идею суверенного интернета

- Мы будем использовать наши кибер-возможности на основе принципов законности, пропорциональности и ответственности, опираясь на четкие механизмы надзора и взаимодействия с населением и союзниками, и мы будем привлекать других к ответственности за безрассудное и неизбирательное поведение в киберпространстве

- Мы будем противодействовать использованию киберпространства в преступных целях всеми доступными средствами, обличая тех, кто прибегает к услугам криминальных посредников или укрывает преступные группировки на своей территории, и мы будем прилагать усилия, чтобы предотвращать распространение высокотехнологичных киберсредств среди преступников

- Мы будем выступать за инклюзивный подход к дебатам о будущем киберпространства и цифровых технологий с участием всех заинтересованных сторон, утверждая права человека в киберпространстве и противодействуя попыткам установления цифрового авторитаризма и государственного контроля

Ключевые изменения в нашем подходе

48. Во многих областях наша стратегия будет опираться на наш текущий подход, направленный на укрепление, расширение и адаптацию наших усилий по мере необходимости. Ниже описаны основные отличия настоящей стратегии от Национальной киберстратегии 2016–2021 года, отражающие наши более масштабные амбиции по укреплению положения Соединенного Королевства как ведущей кибердержавы.

49. Обязательство по сохранению положения Соединенного Королевства на передовых рубежах кибертехнологий. В течение следующих трех лет правительство вложит 2,6 млрд фунтов стерлингов в киберпотенциал и замену устаревших ИТ-систем. Это в дополнение к крупным инвестициям в Национальные силы кибербезопасности, анонсированным в Обзоре расходов 2020 года (SR20). Сюда входят дополнительные 114 млн на финансирование Программы национальной кибербезопасности, а также анонсированное увеличение инвестиций в сферы научно-исследовательских и опытно-конструкторских работ (НИОКР), разведки, обороны, инноваций, инфраструктуры и квалифицированных кадров, — каждая их которых вносит свой вклад в наращивание кибермощи Соединенного Королевства. Инвестиции в киберпотенциал, анонсированные в Обзорах расходов 2020 и 2021 годов намного превышают 1,9 млрд фунтов стерлингов, выделенных в течение пяти лет на реализацию предыдущей стратегии.[19]

50. Более широкомасштабная Национальная киберстратегия. Кибербезопасность по-прежнему лежит в основе этой стратегии, но теперь в ней объединен весь спектр возможностей Соединенного Королевства, имеющийся в правительстве и за его пределами. Она придает большее значение критическим технологиям и инфраструктуре, лежащим в основе киберпространства, а также направлена на предоставление поддержки британским киберкомпаниям в развитии на внутреннем уровне и конкуренции на международном рынке, активизацию международной деятельности по формированию будущего киберпространства и влиянию на него и на интеграцию наступательного киберпотенциала в качестве одного из рычагов власти. Это требует по-настоящему целостного национального стратегического подхода. Настоящая стратегия распределяет обязанности в области лидерства и координации между государственными министрами, и предусматривает гораздо более тесное взаимодействие с автономными администрациями. Это опирается на наш успех в координации усилий в масштабах всего правительства, что является одной из основных сильных сторон Соединенного Королевства.

[19] Министерство финансов Соединенного Королевства, Autumn Budget and Spending Review 2021 (2021)

51. Усилия всего общества. Нам нужен национальный стратегический подход, который формируется при участии организаций по всей стране и помогает им принимать решения; и который служит основой для более тесного сотрудничества с нашими партнерами в Соединенном Королевстве и во всем мире. Чтобы претворить это в реальность, еще многое предстоит сделать. Краткосрочные меры будут включать в себя: (i) образование нового Национального консультативного совета по кибербезопасности, в рамках которого ведущие лидеры частного и третьего секторов будут принимать участие в критической оценке, поддержке и определении нашего подхода; (ii) переориентация инновационных программ в киберсекторе, с переходом от крупных, зачастую базирующихся в Лондоне инициатив к модели осуществляемых на региональном уровне программ, разрабатываемых в партнерстве с местными отраслевыми предприятиями, новаторами, правоохранительными органами и научными кругами и (iii) применение мер по расширению кадрового многообразия в кибер-секторе — признавая, что способность к использованию и развитию квалифицированных и перспективных кадров из всех слоев населения имеет критическое значение для нашей национальной безопасности. Сама стратегия была разработана при участии автономных правительств Северной Ирландии, Шотландии и Уэльса, представителей отрасли, правоохранительных и регулирующих органов, научных кругов, гражданского общества и международных партнеров. Мы намерены поддерживать открытый диалог в продолжение всего периода ее имплементации.

52. Более инициативный подход к укреплению и защите нашего конкурентного преимущества в области технологий, имеющих критическое значение для киберпространства. Начало применению этого подхода в таких областях, как искусственный интеллект, квантовые технологии и данные, уже было положено Интегрированным обзором и последующими стратегиями. Настоящая стратегия содержит дальнейшие обязательства в области проектирования надежных микропроцессорных систем, безопасности операционных технологий и криптографии. Она анонсирует образование национальной лаборатории по безопасности операционных технологий в качестве нового центра передового опыта, деятельность которого сосредоточена на достижении высочайшего уровня киберустойчивости в партнерстве с отраслевыми предприятиями и научными организациями. Она также анонсирует расширение исследовательских возможностей Национального центра кибербезопасности (NCSC), в том числе создание нового центра прикладных исследований в Манчестере, ориентированного на развитие нарождающихся технологий в таких областях как «умные города» и транспорт. Стратегия также опирается на успехи нашей работы в продвижении подходов, требующих интеграции безопасности в новые технологии на стадии проектирования, то есть «безопасные по дизайну» технологии. Это означает вложение средств в разработку и более широкое использование регуляторных и правовых рычагов там, где это необходимо для продвижения более диверсифицированных, защищенных и устойчивых цепочек технологических поставок, как мы это сделали в сфере телекоммуникаций.

53. Значительная активизация ключевых усилий, направленных на продвижение кибербезопасности под руководством правительства. Мы вложим больше средств, чем когда-либо, в оперативное и кардинальное преобразование правительственной системы кибербезопасности, устанавливая четкие стандарты для министерств и ведомств и заменяя унаследованную ИТ-инфраструктуру. К 2025 году будет значительно повышена устойчивость государственной критической инфраструктуры к кибератакам, и мы обеспечим, чтобы к 2030 году все правительственные организации по всему государственному сектору были устойчивыми к известным уязвимостям и видам атак. Мы сделаем еще больше, чтобы защитить и вовлечь наших граждан, по возможности уменьшая бремя, которое ложится на них. Мы повысим устойчивость цифровой среды, защищая граждан от киберпреступности и мошенничества и возлагая еще большую ответственность на производителей, ритейлеров, поставщиков услуг и государственный сектор за повышение стандартов кибербезопасности. Мы будем содействовать повышению уровня вовлеченности и инвестиций частного сектора в киберустойчивость путем согласования правил и стимулов

в масштабах всей экономики и обеспечения еще большей поддержки. Мы также сосредоточим больше усилий на рисках для цепочек поставок, тестируя широкий спектр мер, чтобы помочь организациям управлять рисками для кибербезопасности, связанными с поставщиками, и обеспечивать использование передовых практик по всей цепочке.

54. Более комплексные и длительные кампании, направленные на подрыв деятельности и сдерживание наших противников, а также на защиту и продвижение интересов Соединенного Королевства в киберпространстве. В этих кампаниях будут задействован более широкий спектр дипломатических, политических и оперативных рычагов в масштабах всего правительства. В значительной мере они будут опираться на создание и расширение деятельности Национальных сил кибербезопасности (NCF), которые будут базироваться в Самсбери в графстве Ланкашир. Мы будем более широко применять возможности NCF для ликвидации угроз со стороны как государственных, так и негосударственных субъектов и для укрепления национальной безопасности Соединенного Королевства в целом. На проведение кампаний будут выделяться средства из новых инвестиций в высокотехнологичные возможности правоохранительных органов на национальном, региональном и местном уровнях. Это поможет нам отражать серьезные угрозы, связанные с атаками программ-вымогателей и действиями все более изощренных кибер-преступников. Мы также продолжим использовать британский режим автономных киберсанкций и процедуру присвоения ответственности, чтобы подвергать наказанию наших противников и обличать виновных во вредоносных и безрассудных атаках.

55. Центральное положение кибермощи во внешнеполитической повестке дня Соединенного Королевства и признание того, что осуществление каждой части стратегии требует международного взаимодействия. Мы укрепим наши ключевые альянсы и привлечем более широкий круг стран к противодействию распространения цифрового авторитаризма. На протяжении нескольких ближайших лет мы увеличим инвестиции в международные программы поддержки партнерских стран, помогая повышать их устойчивость и укрепляя их способность противодействовать киберугрозам. Мы будем более эффективно использовать весь спектр наших внутренних достижений, включая опыт, накопленный в области оперативных и стратегических коммуникаций, интеллектуальное лидерство, торговые связи и промышленные партнерства, для поддержки наших международных целей.

Распределение ролей и обязанностей в британском обществе

56. Центральное место в нашей стратегии будет занимать подход к кибербезопасности, основанный на усилиях всего общества. Мы должны построить долгосрочное и сбалансированное партнерство с государственным, частным сектором и третьим сектором, при этом каждый из них будет играть важную роль в общенациональных усилиях.

Граждане

57. Настоящая стратегия призвана как можно больше облегчить бремя киберзащиты, которое ложится на граждан, однако каждый из нас будет и далее играть важную роль. Хотя правительство будет прилагать максимум усилий для того, чтобы останавливать кибератаки до того, как они нанесут ущерб людям, некоторые субъекты угроз найдут способ обойти эти меры защиты. Мы все можем предпринять меры для повышения безопасности активов, которые мы ценим, как в физическом, так и в виртуальном мире.[20] Это потребует от нас выполнения персональных обязанностей по принятию разумных мер для защиты не только оборудования — смартфонов и других устройств, — но и данных, программного обеспечения и систем, которые обеспечивают для нас необходимую свободу, гибкость и удобство в частной и профессиональной жизни. В этих целях правительство предоставляет технически точные, своевременные и практически выполнимые рекомендации. Организации гражданского общества и общественные группы также играют важную роль, помогая людям понять киберриски и защититься

[20] Cyber Aware — рекомендации правительства по обеспечению безопасности в интернете

от них. Многие благотворительные организации, например, предоставляют адресную поддержку и рекомендации уязвимым группам населения и повышают их осведомленность.

Компании и организации

58. Компании и организации обязаны обеспечить эффективное управление своими киберрисками, чтобы повысить киберустойчивость и оказывать поддержку своим клиентам и людям, которые пользуются их услугами. Деятельность, инновационность и рост компаний и организаций все более зависит от цифровых технологий и онлайн-сервисов. Они повышают эффективность услуг, но вместе с тем создают новые риски и вызовы, как например постоянно растущий объем персональных данных и цифровых активов, за которые они отвечают. Это влечет за собой обязанность защищать эти данные и активы, обеспечивая при этом эффективное предоставление услуг. Неспособность сделать это может иметь серьезные репутационные и экономические последствия для организаций и нанести ущерб их клиентам. Операторы жизненно важных услуг и поставщики ключевых цифровых услуг (таких как облачные сервисы), должны, в частности, принимать меры в отношении киберрисков, которые стоят перед ними, и выполнять обязанности, определенные в Положениях о сетях и информационных системах («Положения NIS»). Советы и рекомендации NCSC служат источником поддержки и помогают всем компаниям и организациям защищать свою информацию, активы и системы. Офис уполномоченного по информации (ICO) также предоставляет организациям рекомендации по выполнению их обязанностей по кибербезопасности согласно Общему регламенту Соединенного Королевства по защите данных.

Сектор кибербезопасности и крупные технологические компании

59. Растущий сектор кибербезопасности Соединенного Королевства играет критически важную роль в реагировании на возникающие киберугрозы и вызовы, которые стоят перед нашей страной. Стремительное распространение подключаемых продуктов и ускорение цифровой трансформации компаний и организаций открывают возможности для роста и инноваций в секторе и создания новых услуг и продуктов. Настоящая стратегия описывает, как правительство будет и далее поддерживать рост британского сектора кибербезопасности и использовать его потенциал и знания, поддерживая и укрепляя наши партнерства. Мы также хотим укреплять более широкие партнерства между научными кругами, техническим сообществом в целом и частным сектором, чтобы обеспечить капитализацию всего потенциала технических знаний и ноу-хау Соединенного Королевства.

60. Крупные технологические компании, поставляющие цифровые услуги, играют критически важную роль в создании безопасной среды для деятельности британских компаний и организаций. Это особенно верно в отношении поставщиков управляемых услуг и платформенных компаний, интегрирующих целый ряд видов деятельности. Они должны обеспечивать, чтобы предлагаемые ими услуги были «безопасными по умолчанию» и не слишком полагались на применение их клиентами мер безопасности. Крупные технологические компании также несут особую ответственность за первоочередное обеспечение собственной кибербезопасности. Все большая зависимость компаний, правительства и общества в целом от облачных и онлайн-сервисов ведет к возникновению новых и уникальных уязвимостей и взаимозависимостей.

Правительство

61. Правительство Соединенного Королевства располагает уникальными возможностями для задействования всего разведывательного потенциала, необходимого для понимания наиболее изощренных угроз, разработки и обеспечения соблюдения законов, установления национальных стандартов и противодействия угрозам со стороны враждебных субъектов, в том числе путем проведения наступательных кибероперациий. Эта стратегия позволит нам вкладывать средства в укрепление нашего национального киберпотенциала. Правительственные министерства и государственные органы также отвечают за защиту своих сетей и систем. Правительство, как держатель большого объема данных и поставщик услуг, принимает строгие меры для защиты своих информационных активов. И, наконец, правительство также имеет важную обязанность по предоставлению гражданам, компаниям и организациям рекомендаций в отношении мер, которые они должны предпринимать для своей защиты в интернете. Сюда входит установление необходимых стандартов, которые ключевые компании и организации обязаны соблюдать, чтобы защитить нас всех.

62. Большинство сфер политики и мер кибербезопасности, описанных в этой стратегии, относятся к вопросам в компетенции правительства, таким как национальная безопасность, иностранные дела, оборона, телекоммуникации, стандарты безопасности продуктов и защита потребителей. Но разработка и реализация этой стратегии также зависит от вклада, действий и инвестиций со стороны **автономных правительств Северной Ирландии, Шотландии и Уэльса**. Это особенно верно в отношении тех областей автономной политики, которые связаны, главным образом, с основополагающими целями «экосистемы» и «киберустойчивости», таких как образование, охрана правопорядка и киберустойчивость определенных критически важных секторов, в том числе государственных секторов этих автономных образований. Координация и сотрудничество в рамках всех четырех наций в составе Соединенного Королевства, имеет огромное значение для достижения наибольшего эффекта в масштабах всей страны. Это требует регулярного и своевременного взаимодействия между Кабинетом министров и другими британскими правительственными ведомствами с одной стороны и их коллегами в Уэльсе, Шотландии и Северной Ирландии с другой стороны в целях обмена информацией о приоритетах и планах. Это также поможет избежать дублирования и поможет с максимальной эффективностью использовать государственные финансовые средства. Автономные правительства будут и далее разрабатывать свои киберстратегии и планы, согласуя их с настоящей государственной стратегией Соединенного Королевства.

Национальный центр кибербезопасности

«Содействие созданию в Соединенном Королевстве самых безопасных условий для жизни и работы в интернете»

Национальный центр кибербезопасности (NCSC) официально был основан в 2017 году в структуре GCHQ в качестве ведущего британского национального органа по вопросам кибербезопасности — обмену знаниями, ликвидации системных уязвимостей и обеспечению руководства по ключевым вопросам национальной кибербезопасности.[21] Создание NCSC позволило упростить правительственные операционные структуры, преобразовать способность Соединенного Королевства к реагированию на киберинциденты национального значения и инициировать развертывание инновационных цифровых услуг, которые помогают автоматически повышать безопасность организаций и людей в интернете.

Мы обеспечиваем, чтобы NCSC был готов к вызовам следующего десятилетия, определяя сохраняющие актуальность возможности и атрибуты, лежащие в основе его работы, финансируя их на постоянной основе и направляя их использование на такие области, в которых, согласно операционному опыту, они дают максимально возможный эффект в национальном масштабе.

Сохраняющие актуальность возможности и атрибуты, лежащие в основе работы NCSC:

- первоклассные технические знания в области связанных с кибербезопасностью дисциплин и специализаций, необходимых Соединенному Королевству;
- уникальное знание текущих и потенциальных киберугроз — намерений и возможностей — британским интересам;
- доступ ко всему диапазону возможностей и полномочий Соединенного Королевства в области национальной безопасности в интересах достижения целей кибербезопасности;
- прямое взаимодействие со специалистами по кибербезопасности в ходе сотрудничества с партнерами в научных кругах и отрасли, а также на международном уровне;
- криптографические возможности и услуги, имеющие критическое значение для защищенности и безопасности интересов Соединенного Королевства на международной арене.

Главные обязанности NCSC согласно новой стратегии:

- **принимать непосредственные меры для сокращения ущерба, причиняемого Соединенному Королевству в результате кибератак** путем обеспечения широкомасштабной защиты с помощью цифровых услуг (например, Активной киберзащиты), содействия технологическому прогрессу, управления реагированием на киберинциденты общенационального значения и — при помощи Национальных сил кибербезопасности (NCF) – непосредственного противодействия кибероперациям наших противников;

[21] Правительство Соединенного Королевства, Национальная стратегия кибербезопасности 2016–2021 гг. (2016): параграф 1.9

- **предоставлять поддержку всем слоям британского общества в обеспечении собственной безопасности** путем предоставления доступа к адресным экспертным услугам и уникальным знаниям, с помощью которых граждане, компании и организации по всему Соединенному Королевству смогут защитить себя и содействовать повышению безопасности в интернете для каждого человека в Соединенном Королевстве;

- **вносить технический вклад в политику правительства Соединенного Королевства и в регулирование наиболее важных вопросов кибербезопасности** путем предоставления стратегическим руководителям в Уайтхолле авторитетной технической поддержки и результатов оценки угроз, выполненной с помощью ключевых возможностей NCSC, а также содействия в разработке и осуществлении нормативных документов и регламентов, направленных на обеспечение цифровой безопасности британских граждан, организаций и интересов;

- **укреплять суверенный потенциал Соединенного Королевства** за счет использования возможностей Национального центра Crypt-Key при NCSC, призванного обеспечивать защиту критически важной информации и услуг, от которых зависит работа британских специалистов в области обороны и национальной безопасности, в том числе защиту от атак со стороны наиболее способных противников;

- **содействовать расширению кадровой базы киберспециалистов и увеличению инвестиций в их подготовку** путем создания технической основы на каждом уровне подготовки киберспециалистов, расширения взаимодействия с отраслью, предоставления поддержки и стимулирования инвестиций в киберсектор.

NCSC будет также вносить вклад в **оценку прогресса** в достижении целей настоящей национальной стратегии силами NCSC Assessments — редакционно независимого функционального подразделения по оценке кибербезопасности.

Национальные силы кибербезопасности

Образованные в 2020 году Национальные силы кибербезопасности (NCF) отвечают за проведение операций в киберпространстве и при его помощи, направленных на противодействие, подрыв, ослабление и борьбу с действиями тех, кто может причинить ущерб Соединенному Королевству или его союзникам, в целях укрепления безопасности страны, а также защиты и продвижения интересов Соединенного Королевства внутри страны и за ее пределами. В состав NCF входит персонал сил обороны и разведки примерно в равном соотношении, что позволяет объединить их опыт, ресурсы и полномочия в рамках единой структуры. Они будут базироваться в Самсбери в графстве Ланкашир.

NCF обеспечивают достижение широкого ряда результатов деятельности в интересах национальной безопасности, такой как содействие обороне, повышение экономического благополучия Соединенного Королевства и предотвращение серьезных преступлений. Деятельность NCF охватывает широкий диапазон мер — от тактических действий до стратегических мер борьбы как с государственными, так негосударственными субъектами. Их деятельность подразделяется на три основные категории:

- противодействие угрозам со стороны террористов, преступников и государств, использующих интернет для проведения трансграничных операций в целях причинения вреда Соединенному Королевству и другим демократическим обществам;
- противодействие угрозам нарушения конфиденциальности, целостности и доступности данных и услуг в киберпространстве (то есть поддержка кибербезопасности);
- поддержка британских оборонных операций и помощь в осуществлении внешней политики Соединенного Королевства (например, реагирование на гуманитарные кризисы в целях защиты гражданского населения).

Операции NCF могут использоваться для оказания влияния на отдельных людей и группы, подрыва онлайновых и коммуникационных систем и нарушения функциональности физических систем. Этот вид деятельности часто называют наступательными кибероперациями (НК).

Операции NCF осуществляются в соответствии с общепризнанными правовыми нормами, включая Закон 1994 года о разведывательных службах и Закон 2016 года о регулировании полномочий следственных органов. Соединенное Королевство ранее четко заявляло, что оно разрабатывает и развертывает возможности в соответствии с международным правом, включая, где применимо, право вооруженных конфликтов. Деятельность NCF подлежит утверждению на министерском уровне, судебному и парламентскому надзору, поэтому британский режим управления кибероперациями — один из самых строгих в мире.

Соединенное Королевство обычно не обсуждает отдельные кибероперации, но можно назвать некоторые виды операционной деятельности, которую могут осуществлять NCF:

- срыв планов террористических групп путем вывода из строя коммуникационных систем передачи команд и управления, а также ограничения распространения экстремистской информации;
- снижение риска причинения вреда британским вооруженным силам путем нарушения функциональности систем вооружения противника;
- защита демократии и свободных, честных и открытых выборов путем противодействия организованным государственным кампаниям дезинформации, направленным на их подрыв;
- препятствие получению криминальными группировками прибыли от своей деятельности путем лишения их возможности пользоваться онлайновыми платформами и сервисами;
- содействие соблюдению международных санкций путем подрыва усилий, направленных на уклонение от них;
- защита Соединенного Королевства и других субъектов от кибератак путем разрушения инфраструктуры, которую противники используют для их осуществления;
- защита гражданского населения в условиях гуманитарного кризиса путем сохранения возможностей для доступа к критически важной информации.

В качестве национального центра передового опыта в проведении операций базовых эффектов в киберпространстве и с его помощью NCF будут способствовать кардинальному улучшению способности Соединенного Королевства развивать, интегрировать и использовать эти кибер-возможности наряду с другими, а также оптимизировать их для достижения нужного эффекта.

Национальная сеть правоохранительных органов по борьбе с киберпреступностью

Созданная в период действия Национальной стратегии кибербезопасности 2016–2021 года национальная сеть правоохранительных органов по борьбе с киберпреступностью разработала планы полномасштабного комплексного реагирования на киберпреступления и готова к развертыванию мер реагирования на основе разведывательных данных в ответ на любые формы кибератак, направленных против людей, организаций и целых секторов. Это национальная система, действующая на национальном, региональном и местном уровнях. В ее задачи входит предоставление поддержки пострадавшим, оказание помощи юридическим и физическим лицам в обеспечении своей безопасности и способности к быстрому восстановлению и повышение действенности уголовного правосудия в отношении преступников.

Национальное подразделение по борьбе с киберпреступностью (NCCU) в структуре Национального агентства по борьбе с преступностью (NCA) выступает в роли национального руководителя и координатора деятельности по реагированию на киберпреступления. Оно опирается на поддержку сети специализированных **региональных подразделений по борьбе с киберпреступностью (RCCU)**, созданных в каждом из девяти полицейских территориальных округов Англии и Уэльса, и действует в партнерстве с коллегами из Служб полиции Шотландии и Северной Ирландии, а также с подразделением по борьбе с киберпреступностью в структуре Службы столичной полиции.

В сеть также входят специализированные **местные подразделения по борьбе с киберпреступностью (LCCU)** в составе каждой из 43 полицейских служб, деятельность которых синхронизирует региональный координатор. Эти региональные и местные подразделения уполномочены осуществлять расследования и преследование правонарушителей, помогать компаниям и потерпевшим защищать себя от атак, а также совместно с партнерами предотвращать вовлечение уязвимых лиц в преступную кибердеятельность.

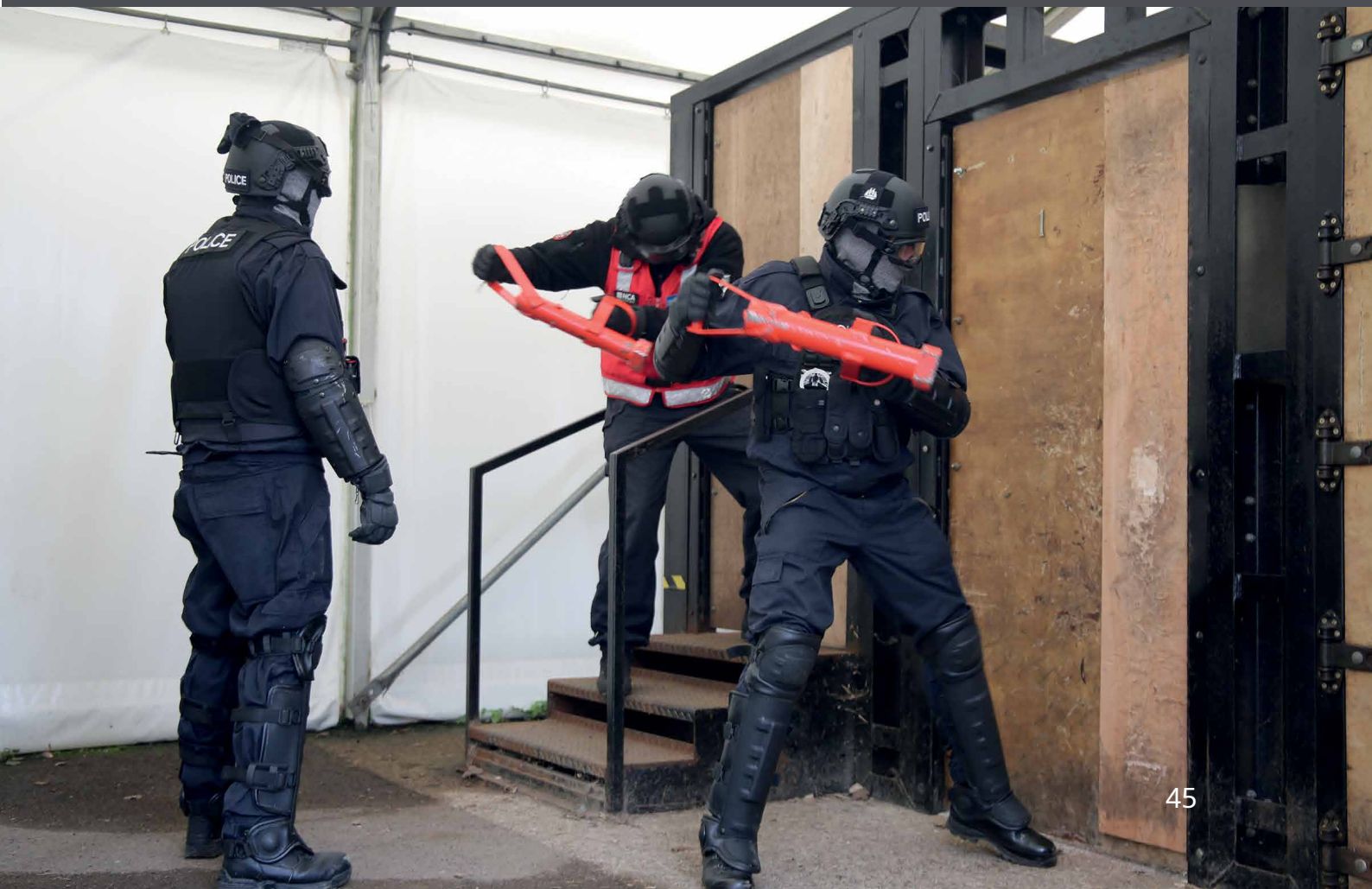
Вопросы централизованной регистрации, классификации и анализа данных о преступности находятся в ведении организации **Action Fraud** при **Службе полиции Лондонского Сити**. Наиболее серьезные и/или сложные случаи затем передаются в NCA и региональную сеть, а менее серьезные — распределяются среди местных служб полиции. Служба полиции Лондонского Сити также координирует оказание поддержки пострадавшим, в том числе силами **Подразделения по работе с жертвами экономических преступлений.**

Объединив системы с качественно новыми возможностями криминалистической экспертизы, разведки и обмена данными, мы создаем единую платформу, с помощью которой национальные и региональные подразделения смогут получать доступ ко всем специализированным высокотехнологичным средствам и инструментам, которые находятся в разработке. Сюда входит способность осуществлять эффективное сотрудничество с партнерами из структур безопасности и разведки, в частности в области реагирования на смешанные криминально-государственные угрозы. Руководствуясь

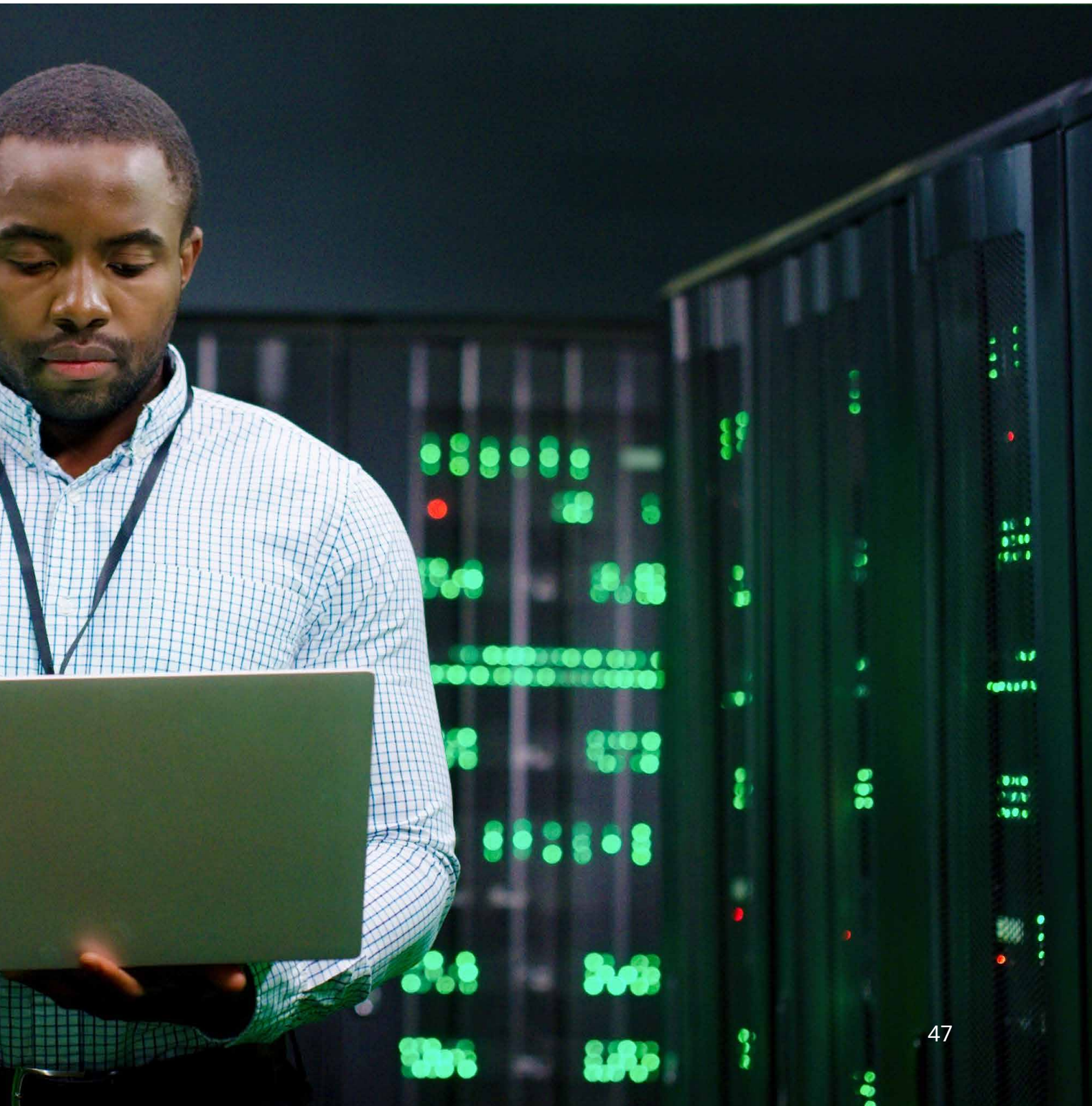
кредо «создать один раз и навсегда, создать на национальном уровне в интересах всей сети борьбы с киберпреступностью», мы даем местным подразделениям по борьбе с киберпреступностью доступ к этим возможностям через региональных координаторов. Этот общесистемный подход уже обеспечивает значительно более эффективное реагирование на угрозы киберпреступности.

Сеть правоохранительных органов по борьбе с киберпреступностью будет и далее содействовать укреплению уголовно-правовых мер борьбы с киберпреступностью, независимо от того, создают ли субъекты угрозы на международном, национальном, региональном или местном уровне.
В дополнение к этому будет применяться ряд других деструктивных методов, в том числе:

- разработка специализированных высокотехнологичных разведывательных и деструктивных кибер-возможностей;
- использование широкой международной сети NCA для поддержки мер, принимаемых партнерскими странами, путем предоставления разведывательных данных и фактической информации;
- препятствие получению криминальными группировками прибыли от своей деятельности путем лишения их возможности пользоваться криминальными рыночными каналами и вспомогательными сервисами;
- защита Соединенного Королевства и других стран от киберпреступлений путем нарушения функциональности и разрушения инфраструктуры, используемой для их осуществления;
- участие в деятельности по введению санкций и публичному присвоению ответственности лицам в высших эшелонах власти;
- конфискация криптовалюты и других активов, являющихся доходами от киберпреступлений.



Часть 2.
Осуществление



Основополагающая цель 1:

кибернетическая экосистема Соединенного Королевства

Укрепление кибернетической экосистемы Соединенного Королевства

63. Для успешного осуществления этой стратегии мы должны обеспечить, чтобы у Соединенного Королевства были необходимые люди, знания и партнеры. Чтобы выйти на лидирующие позиции в области критических технологий, нам нужны разнообразные высококвалифицированные технические кадры, активное научное сообщество, конкурентоспособный на международном уровне киберсектор и процветающая региональная экосистема инноваций — и все это на основе более крепких партнерских отношений между правительством, отраслью и научными кругами.

64. Кибернетическая экосистема должна быть самодостаточной и не зависеть от государственного вмешательства. В период действия настоящей стратегии мы осуществим переход от финансирования преимущественно индивидуальных, централизованно управляемых программ подготовки квалифицированных кадров и инноваций к более устойчивому и системному региональному подходу. Опираясь на широкие государственные реформы систем профессиональной подготовки и образования, мы будем оказывать поддержку молодым людям в получении навыков, необходимых для карьеры в киберсекторе и стимулировать их интерес к этой профессии. Мы будем отдавать приоритет комплексу конкретных мер по повышению многообразия кадровой базы киберспециалистов. Речь идет не только о том, чтобы эти рабочие места и карьерные возможности были доступны для каждого. Для обеспечения национальной безопасности критически важно использовать потенциал талантливых и квалифицированных кадров из всех слоев населения. Мы также обеспечим, чтобы преимущества роста киберсектора были доступны для всего Соединенного Королевства, а не только для Лондона и Юго-Востока страны, на которые приходится 45% рабочих мест этого сектора и 85% внешних инвестиций.[22]

65. В целом, мы будем играть более стратегическую роль, содействуя объединению усилий лидеров отрасли, ученых, новаторов, правоохранительных органов, органов национальной безопасности и других лиц и организаций, готовых вместе работать над повышением устойчивости Соединенного Королевства к киберугрозам. Мы объединим все государственные рычаги для поддержки кибернетической экосистемы, начиная с методов преподавания основ кибербезопасности в школах и заканчивая повышением стандартов с помощью экономических рычагов регулирования, чтобы обеспечить наращивание Соединенным Королевством жизненно важного потенциала, необходимого для защиты государства от будущих киберугроз.

[22] Министерство цифровизации, культуры, СМИ и спорта, Cyber Security Sectoral Analysis 2021 (2021)

Задача 1. Укреплять структуры, партнерства и сети, необходимые для поддержки подхода к кибербезопасности, основанного на усилиях всего общества

66. Для наращивания кибермощи необходимы усилия всего общества. Наше конкурентное преимущество будет обеспечено способностью развивать и использовать перспективные кадры во всем Соединенном Королевстве и привлекать необходимых специалистов из государственного сектора, отрасли и научных кругов к совместной работе с использованием необходимых методов, поддерживая объединение усилий всего сообщества кибербезопасности. Нам потребуется создать по-настоящему интегрированное, ориентированное на результаты партнерство с отраслью и применить широкий географический подход к объединению усилий всех наций и регионов Соединенного Королевства в тесном сотрудничестве с автономными правительствами Северной Ирландии, Шотландии и Уэльса, чтобы обеспечить выравнивание возможностей, условия для которого создает киберпотенциал. К 2025 году мы достигнем следующих результатов:

67. Более инклюзивный и стратегический национальный диалог по вопросам кибербезопасности с участием отрасли, научных кругов и граждан, который опирается на новый Национальный консультативный совет по кибербезопасности, уже прочные сети партнерских организаций в области наращивания киберпотенциала и укрепления устойчивости и на центры передового академического опыта в области исследования вопросов кибербезопасности и обучения.

68. Более интегрированные и эффективные региональные сети организаций по кибербезопасности по всему Соединенному Королевству, которые содействуют укреплению партнерских отношений между правительством, компаниями и научными кругами, поддерживая развитие сектора и повышение устойчивости бизнеса. Мы будем работать вместе с региональными кибер-кластерами и недавно образованной организацией UK Cyber Cluster Collaboration (UKC3), а также с растущим числом региональных центров кибер-инноваций и Центров киберустойчивости, над укреплением связей между местными компаниями, центрами передового академического опыта и правоохранительными органами.

69. Эти шаги будут опираться на существующие широкие связи между Национальным центром кибербезопасности (NCSC) и заинтересованными лицами, между правительственными ведомствами, независимыми структурами и секторами экономики, которые они представляют, включая объекты критической национальной инфраструктуры и регулирующие органы, а также на более широкий диалог правительства с отраслью и цифровым и технологическим секторами.

Киэра Митчелл, глава подразделения ScotlandIS

Киэра также является менеджером Кибер-кластера Шотландии и членом правления UKCI3.

«Кибер-кластер Шотландии играет ключевую роль в поддержке сообщества кибербезопасности в Шотландии. Растет понимание опыта управления кластерами, накопленного Шотландией, и возможностей для развития процветающего киберсектора. На фоне растущего признания ценности кластеров я с радостью приняла назначение на ключевую роль в новой организации UK Cyber Cluster Collaboration — руководитель по развитию экосистемы. В рамках своей деятельности UKCI3 будет уделять особое внимание сотрудничеству, инновациям и повышению квалификации специалистов, чтобы обеспечить платформу для роста британского сектора кибербезопасности».

Кибероорганизации (местонахождение указано ориентировочно)

Британские кибер-кластеры

1. Кибер-кластер Бристоля и Бат
2. Кибер-кластер Севера
3. Кибер-кластер Уэльса
4. CyNam (Кибер-кластер Челтнема)
5. Восточно-английский кластер кибербезопасности
6. Мидлендский кибер-кластер
7. Кибер-кластер ScotlandIS
8. Юго-западный кластер кибербезопасности
9. Йоркширский кластер кибербезопасности
10. Кибер-кластер NI (Северная Ирландия)
11. Северо-западный кластер кибербезопасности
12. Западно-английский кибер-кластер

- Академический центр передового академического опыта в области кибербезопасности
- Академический центр передового исследовательского опыта в области кибербезопасности
- Место нахождения GCHQ / NCSC
- Организации автономных администраций

* Красными точками с черной линией обозначены учреждения, имеющие как академический, так и исследовательский статус

1 Центр бизнес-устойчивости для северо-восточного региона

2 Центр киберустойчивости северо-западного региона

3 Центр киберустойчивости для региона Ист-Мидлендс

4 Центр киберустойчивости для региона Уэст-Мидлендс

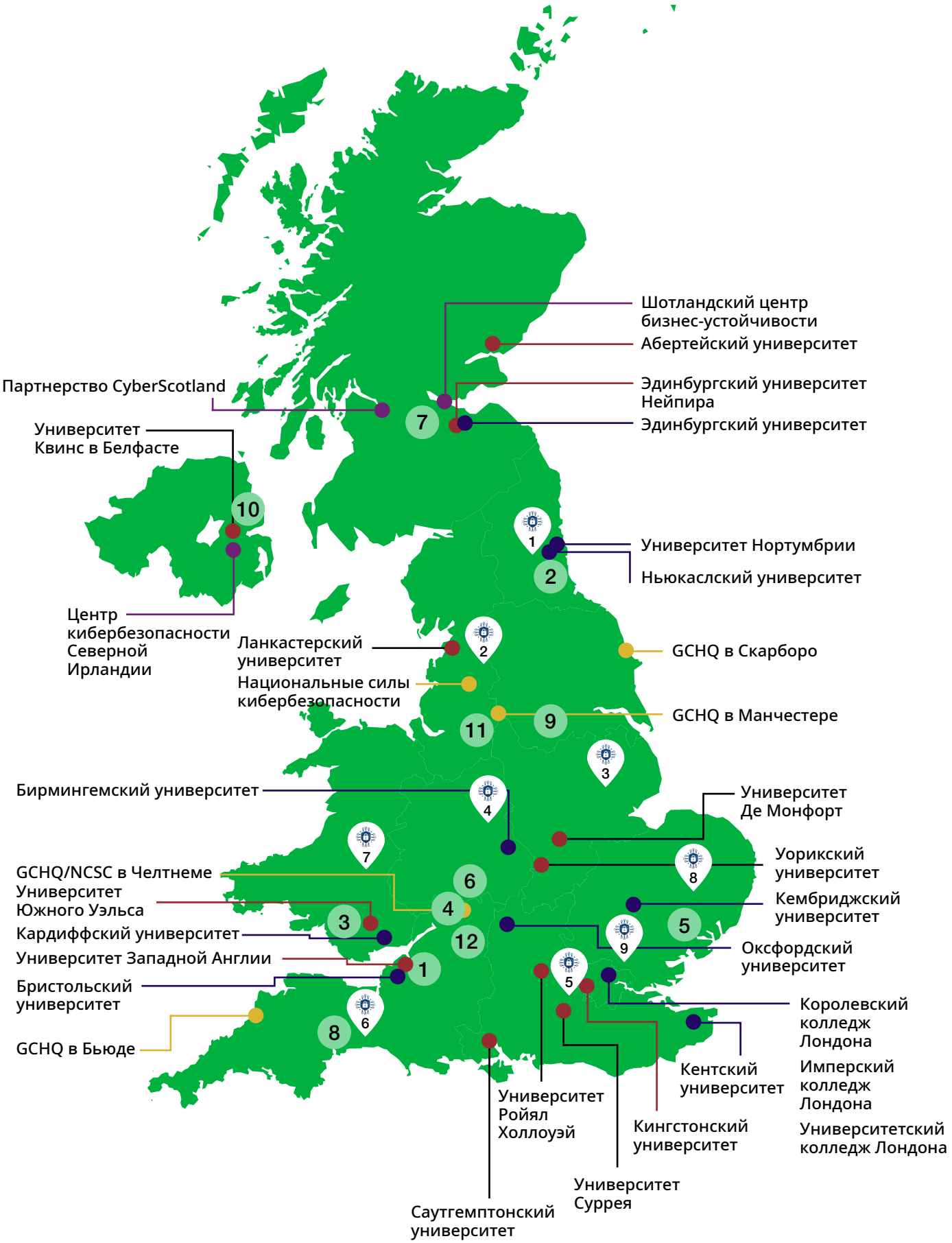
5 Центр киберустойчивости для Юго-Восточного региона

6 Юго-Западный центр киберустойчивости

7 Центр киберустойчивости для Уэльса

8 Восточный центр киберустойчивости

9 Центр киберустойчивости для Лондона


Шотландский центр бизнес-устойчивости
Абертейский университет
Партнерство CyberScotland
Эдинбургский университет Нейпира
Эдинбургский университет
Университет Квинс в Белфасте
Университет Нортумбрии
Ньюкаслский университет
Центр кибербезопасности Северной Ирландии
Ланкастерский университет
GCHQ в Скарборо
Национальные силы кибербезопасности
GCHQ в Манчестере
Бирмингемский университет
Университет Де Монфорт
Уорикский университет
GCHQ/NCSC в Челтнеме
Университет Южного Уэльса
Кембриджский университет
Кардиффский университет
Оксфордский университет
Университет Западной Англии
Бристольский университет
Королевский колледж Лондона
GCHQ в Бьюде
Кентский университет
Имперский колледж Лондона
Университет Ройял Холлоуэй
Кингстонский университет
Университетский колледж Лондона
Университет Суррея
Саутгемптонский университет

Задача 2. Укреплять и расширять кадровую базу квалифицированных киберспециалистов на всех уровнях, в том числе путем повышения престижа разносторонней профессии специалиста по кибербезопасности мирового класса, которая вдохновляет и привлекает будущие перспективные кадры.

70. Центральное значение для достижения целей Соединенного Королевства будет иметь создание устойчивых и диверсифицированных источников пополнения кадрового резерва в киберсекторе высококвалифицированными специалистами, способными обеспечивать безопасность ключевых элементов цифровой экономики, а также развивать инновации и разрабатывать новые подходы. Это будет содействовать достижению нашей цели — служить примером для подражания, признавая и сохраняя опыт и знания в масштабах всего государственного сектора и расширяя наши возможности в сферах охраны правопорядка, обороны и безопасности, включая Национальные силы кибербезопасности (NCF). Так же как и в случае других составляющих настоящей стратегии, мы будем сотрудничать с автономными правительствами Шотландии, Уэльса и Северной Ирландии, чтобы обеспечить последовательность общенационального подхода к британским правительственным инициативам в областях, которые находятся в ведении автономных правительств, таких как образование и подготовка квалифицированных кадров. К 2025 году мы достигнем следующих результатов:

71. Значительное увеличение числа людей, имеющих необходимую квалификацию для пополнения кадрового резерва киберспециалистов, которое опирается на деятельность в масштабах всех четырех наций в составе Соединенного Королевства, направленную на согласование политики в области образования и подготовки квалифицированных кадров с требованиями персонала и работодателей. В этих целях мы примем ряд мер, в том числе по расширению программ подготовки для лиц старше 16 лет в соответствии с потребностями в развитии кадрового резерва в области кибербезопасности, финансируя учебные лагеря по развитию навыков кибербезопасности, реализуя на национальном уровне программу Институтов технологий и продолжая поддерживать Программу стипендий CyberFirst для студентов. Эта деятельность будет опираться на усилия правительства, направленные на согласование к 2030 году большинства программ обучения и подготовки лиц старше 16 лет с более строгими стандартами, установленными по инициативе работодателей. Стандарты будут разработаны в сотрудничестве с британским Советом по кибербезопасности для использования в киберсекторе и в целом и лягут в основу программ профессиональной подготовки, квалификации уровня T и новых, более высоких технических квалификаций. Это позволит работодателям играть центральную роль в планировании и разработке программ квалификации и подготовки.

72. Более качественная, утвердившаяся, признанная и формализованная профессия специалиста по кибербезопасности. Опираясь на результаты работы передового проекта Cyber Security Body of Knowledge (CyBOK), Британский Совет по кибербезопасности, получивший Королевскую грамоту, установит профессиональные стандарты и пути для выбора карьеры и продвижения по службе в киберсекторе. Мы будем использовать все государственные рычаги, включая законодательство, для интеграции этих стандартов в масштабах профессии, обеспечивая четкое и последовательное признание передовых знаний и опыта в рамках всей кадровой базы в киберсекторе.

73. Более многообразная кадровая база киберспециалистов, более эффективная поддержка людям из недостаточно представленных и неблагополучных групп населения в Соединенном Королевстве в выборе карьеры и успешной работе в киберсекторе. Эти меры предусматривают оказание содействия большему числу женщин в выборе карьеры в киберсекторе и специальной поддержки недостаточно представленным группам населения в продвижении по службе до высоких руководящих должностей. Мы будем развивать успехи, достигнутые в ходе проведения внешкольных мероприятий в рамках флагманской программы CyberFirst, включая конкурс CyberFirst среди девочек. Мы также расширим доступ молодых людей в группах риска к возможностям для получения образования и карьерного роста, которые открывает участие в программе Cyber Choices Национального агентства по борьбе с преступностью, отвращая их от участия в незаконной кибердеятельности и поощряя к использованию положительных возможностей для применения своего таланта и энтузиазма.

74. Стабильный выпуск разнообразных высококвалифицированных специалистов из учреждений в системе образования. Мы будем поощрять и поддерживать молодых людей, стремящихся получить техническое образование, в том числе увеличим набор и многообразие кандидатов для изучения предмета «Компьютерные науки» в средней школе (по системе GCSE) и для получения эквивалентной квалификации в Шотландии, а также увеличим возможности в области высшего и профессионального образования, например квалификации Уровня T в Англии, и ученичества. Кроме того, мы будем содействовать повышению квалификации учителей в Англии при поддержке Национального центра компьютерного образования (NCCE), который обеспечит им доступ к ресурсам и возможностям для профессионального развития, помогая стимулировать интерес среди студентов.

75. Правительство более эффективно подбирает, нанимает, обучает и удерживает киберспециалистов, которые ему требуются. Как крупные работодатели для киберспециалистов, правительство и государственный сектор должны собственным примером демонстрировать поддержку и активизацию мер, описанных выше. Мы будем применять более последовательный и эффективный подход в масштабах всего государственного сектора, а также принимать конкретные индивидуальные меры для повышения квалификации гражданских служащих и руководителей высшего звена и наращивать наш потенциал в сфере обороны и безопасности, включая укрепление NCF, NCSC и правоохранительных органов. Сюда входят инвестиции в подготовку молодых талантов путем расширения охвата инициативы Cyber Fast Stream и программ ученичества в области кибербезопасности, поддержка программ развития специализированных навыков в рамках NCA, включая создание рабочих мест для выпускников и стажеров, специализированные программы поддержки нейроразнообразия и летние программы поддержки многообразия. Опираясь на успех Школы кибероборонs, мы создадим на ее основе Академию кибероборонs с расширенными учебными программами по оборонительным и наступательным кибероперациям, вместе с тем укрепляя сотрудничество с научными, отраслевыми и международными партнерами.

Британский Совет по кибербезопасности

Британский Совет по кибербезопасности был создан в марте 2021 года и представляет собой первую в мире профессиональную организацию в области кибербезопасности. Его миссия — представлять интересы этой профессии, обеспечивая прозрачность и структуризацию растущей кадровой базы киберспециалистов и всего спектра квалификаций, сертификатов и дипломов в этой области. Это важный шаг, способствующий признанию того, что профессия киберспециалиста, так же как давно сложившиеся профессии в области медицины и права, включает в себя широкий ряд технических и нетехнических компетенций и специализаций во всех секторах экономики.

Совет преследует цели в следующих четырех областях:

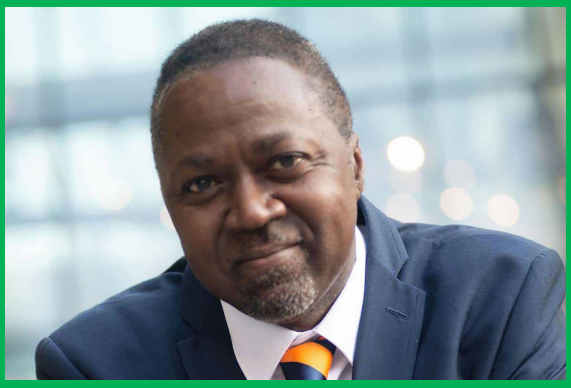
- идейное руководство и профессиональные стандарты: руководство работой по разработке и утверждению стандартов, определяющих кибербезопасность;
- профессиональная карьера и обучение: оказание поддержки работодателям и отдельным людям в принятии решений о выборе карьеры, предоставление рекомендаций по квалификациям в области кибербезопасности, профессиональному развитию и признанию;
- профессиональная этика: разработка руководящих принципов, опираясь на которые практикующие специалисты и организации могут продемонстрировать соблюдение ими этических норм в области кибербезопасности;
- многообразие и инклюзивность: продвижение карьерных возможностей в области кибербезопасности для людей любого возраста и социального происхождения, содействие устранению препятствий для выбора этой карьеры и продвижения по службе.

Совет будет стремиться к утверждению и укреплению своего авторитета и устойчивости как профессиональной организации в течение всего срока действия этой стратегии. Он объединит под своей эгидой целый ряд существующих профессиональных и сертификационных органов, определяя и расширяя возможности экспертных организаций, которые смогут четко обозначить требования к продвижению по службе и компетенциям для новых и давно работающих сотрудников, а также для работодателей.

Королева утвердила предоставление Британскому Совету по кибербезопасности Королевской грамоты в ноябре 2021 года. Впервые в истории это обеспечило признание профессии специалиста по кибербезопасности, которая охватывает ряд специализаций, существующих в этой области.

Мы понимаем, что многое еще предстоит сделать, чтобы закрепить профессиональные стандарты и пути профессионального развития в масштабах всей кибернетической экосистемы, в том числе в государственном, оборонном и правоохранительном секторах. Совет будет играть в этом важную роль, помогая молодым и желающим сменить профессию людям понять, какие существуют возможности для карьеры в киберсекторе.

Саймон Хепберн, CEO, Британский Совет по кибербезопасности



Моя работа связана с продвижением Британского Совета по кибербезопасности как «авторитетной профессиональной организации в области кибербезопасности». Совет — британский орган профессионального саморегулирования в области кибербезопасности. Мы стремимся объединить усилия отрасли, направленные на разработку, продвижение и утверждение признанных на национальном уровне стандартов в киберсекторе, содействуя созданию в Соединенном Королевстве самых безопасных условий для жизни и работы в интернете. Совет официально приступил к работе в марте 2021 года по успешном завершении проекта по его образованию и уже открыт для приема заявлений о членстве. Национальная киберстратегия — один из ключевых элементов, которые позволяют гражданам и организациям осуществлять деятельность таким образом, чтобы содействовать развитию этой профессии, и Совет играет в этом ведущую координирующую роль.

Задача 3. Активизировать рост устойчивого, инновационного и конкурентоспособного на международном уровне сектора информационной и кибербезопасности, поставляющего качественные продукты и услуги в соответствии с потребностями государства и экономики в целом

76. Для укрепления национальной кибермощи и стимулирования роста цифровой экономики и экспорта Соединенному Королевству требуется активный киберсектор, представленный солидными и надежными компаниями. Британские фирмы поставляют ведущие в мире технологии и услуги по обучению и консалтингу как отраслевым, так и государственным организациям в Соединенном Королевстве и за рубежом. Однако, чтобы иметь возможности для развития передовых технологий и перехода к этапу выпуска жизнеспособного продукта, некоторым компаниям требуется поддержка и контакты с инвестиционными организациями.

77. Компаниям также нужна уверенность в том, что они разрабатывают инновации в соответствии с утвержденными правительством параметрами, которые также соблюдают другие организации. Мы можем сделать больше, чтобы помочь покупателям ориентироваться в этом сложном разнообразии продуктов и услуг разного качества. Это, в свою очередь, будет стимулировать спрос в экосистеме и содействовать дальнейшему росту. К 2025 году мы достигнем следующих результатов:

78. Киберсектор, рост которого из года в года превышает средние темпы мирового роста, в том числе благодаря торговле и экспорту продуктов и услуг в области кибербезопасности. Мы будем содействовать доступу компаний киберсектора к новым рынкам как внутри страны, так и за рубежом, поддерживая проведение в Соединенном Королевстве первоклассных флагманских мероприятий в сфере кибербезопасности и приглашая наиболее инновационные киберкомпании к участию в торговых миссиях и международных торговых ярмарках в этой области. Мы будем более эффективно использовать возможности в сфере государственных закупок и создадим всеобъемлющий каталог поставщиков, аккредитованных NCSC, в целях поощрения спроса на высококачественные продукты и услуги по кибербезопасности.

79. Еще более высокий уровень инноваций в киберсекторе, при увеличении объемов инвестиций на ранних этапах и росте числа киберкомпаний, которые смогли успешно начать работу, развиваться и расширять свою деятельность. Роль единого координационного центра для поддержки компаний будет играть программа Cyber Runway, созданная с учетом опыта осуществления предыдущих программ, таких как Tech Nation Cyber Programme, Cyber101 и Hut Zero. Мы преобразуем Челтнемский инновационный центр, включая акселератор для кибербизнеса «NCSC for Startups», в поистине международный центр инноваций — Национальный центр киберинноваций. Мы будем опираться на экспертные знания и опыт организаций, которые уже занимаются поощрением и стимулированием сотрудничества, таких как Биржа технологий и инноваций в области национальной безопасности. Мы будем поощрять рискованные вложения на начальных стадиях работы стартапов, в том числе за счет средств Фонда стратегических инвестиций в национальную безопасность и в партнерстве с Британским Бизнес Банком

80. В киберэкономике Соединенного Королевства наблюдается значительное выравнивание возможностей на фоне ускорения роста за пределами Юго-Востока страны, что содействует восстановлению страны от последствий пандемии коронавируса (COVID-19) и поддерживает региональную экономическую деятельность в целом. Мы создадим постоянный штаб NCF в Самсбери на северо-западе Англии, стимулируя развитие технологий, цифровой сферы и оборонного сектора за пределами Лондона и содействуя созданию новых партнерств в этом регионе. Мы будем активнее помогать новаторам и предпринимателям за пределами Лондона и Юго-Востока разрабатывать продукты и услуги, развивать их бизнес и подбирать квалифицированные кадры. Сюда входит кампус Golden Valley, который работает под руководством Городского совета Челтнема и нацелен на содействие росту компаний, связанных с кибертехнологиями. Мы будем содействовать наращиванию экспортного потенциала киберкомпаний в других регионах Соединенного Королевства путем взаимодействия с региональными кибер-кластерами и организации отдельных мероприятий для демонстрации международным покупателям возможностей наших талантливых специалистов в киберсекторе.

81. Возросшее число компаний, способных поставлять технологии, продукты и услуги в области кибербезопасности, которые отвечают независимо проверенным стандартам качества и пользуются повышенным доверием пользователей. Мы будем обеспечивать это в соответствии с официальным документом «The Future of NCSC Technology Assurance», опубликованным NCSC в сентябре 2021 года, используя бренд и опыт NCSC для формирования надежного рынка, чтобы помочь британским потребителям покупать услуги с уверенностью в их надежности, повышать свою безопасность и поднять планку национальной кибербезопасности.[23]

[23] NCSC, Официальный документ: The future of NCSC Technology Assurance (2021)

Берта Паппенхейм, CEO и основатель, Cyberfish Company

CyberFish принимала участие в государственной программе акселерации кибербизнеса. Наша миссия заключается в том, чтобы помогать компаниям и правительству повышать эффективность реагирования на сбои в работе, например, в результате киберинцидентов. С этой целью мы организуем совместные учения с имитацией инцидентов, наблюдаем за динамикой работы команд в условиях стресса и даем рекомендации по достижению улучшений. Многие советники хорошо знакомы либо с технической стороной реагирования на инциденты, либо с поведенческими аспектами лидерства и принятия решений. Мы умеем эффективно делать и то, и другое, и обладаем экспертными знаниями в обеих областях. Благодаря проводимым нами учениям уже почти 500 передовых отраслевых предприятий, выполняющих критически важные задания по всему миру, добились перемен в подходах и повысили результативность работы в группах, что позволило повысить эффективность реагирования на кризисы и принятия решений.

Хотите влиться в ряды киберспециалистов или начать свой бизнес?

82. В нашей предыдущей стратегии основное внимание уделялось наращиванию базы квалифицированных кадров и развитию сектора услуг кибербезопасности в Соединенном Королевстве.
Как описывается в разделе о стратегическом контексте, мы добились значительного прогресса в **развитии киберсектора и увеличении экспорта**:

Содействие киберкомпаниям в выходе на международные рынки. Объем экспорта услуг кибербезопасности из Соединенного Королевства составил 4,2 млрд фунтов стерлингов в 2020 году.

Cyber Exchange — интернет-портал, поддерживающий взаимодействие киберкомпаний изо всех регионов Соединенного Королевства.

Инициатива Cyber Growth Partnership объединяет усилия правительства и отрасли, направленные на устранение препятствий для роста.

83. Мы оказываем **поддержку новаторам, помогая им развивать и расширять свой бизнес и** обеспечивая процветание британской кибернетической экосистемы в течение последних пяти лет:

NCSC for Startups помогает инновационным компаниям ориентироваться в самых важных стратегических вызовах, при этом стартапы уже принимают участие в более чем 160 новых корпоративных испытаниях.

LORCA помогла 72 инновационным компаниям в киберсекторе привлечь инвестиции в сумме более 200 миллионов фунтов стерлингов и получить доход в размере более 37 миллионов фунтов стерлингов.

Cyber Runway помогает инновационным компаниям в основании, развитии и расширении масштабов бизнеса, опираясь на успехи таких инициатив, как Hutzero и Cyber101.

84. Мы работаем над сокращением дефицита **новых работников в киберсекторе**, составляющего 10 тысяч человек в год:[24]

Программа предоставления стипендий CyberFirst направлена на оказание поддержки студентам, и благодаря ей сотни граждан, уже имеющих опыт работы, ежегодно пополняют ряды киберспециалистов.

На сегодняшний день в киберсекторе существуют четыре стандарта ученичества, разработанные силами отрасли, и три варианта первичной подготовки в рамках инициативы «Courses for Jobs» под эгидой министерства образования.

Было организовано девять учебных лагерей по развитию навыков кибербезопасности при поддержке недавно созданного Национального фонда развития профессиональных навыков, которые открывают для участников интересные карьерные возможности в киберсекторе; на каждый год следующего расходного периода запланировано еще больше таких мероприятий.

85. Мы работаем над **приданием официального статуса профессии киберспециалиста**, помогая организациям понять, специалисты какой квалификации им требуются, а гражданам — ориентироваться в необходимой информации:

Британский Совет по кибербезопасности — одна из первых в мире авторитетных профессиональных организаций в области кибербезопасности. Он начал разработку четких и последовательных профессиональных стандартов, опираясь на весь объем работы, проделанной существующими профессиональными организациями до сегодняшнего дня. Совет займется четким определением эффективных квалификаций из огромного числа квалификаций, доступных в настоящее время.

The Cyber Security Body of Knowledge (CyBOK) занимается подготовкой материалов и поддержкой учебной и профессиональной подготовки в секторе кибербезопасности.

[24] Министерство цифровизации, культуры, СМИ и спорта, Understanding the cyber security recruitment pool (2021)

86. Мы работаем над тем, чтобы **возможность работать в киберсекторе была доступна для всех людей**, устраняя неравенство в секторе, в котором лишь 16% кадровой базы составляют женщины и лишь 3% женщин и представителей этнических меньшинств занимают высшие руководящие должности.[25]

За последние пять лет в курсах CyberFirst и программе Discovery приняли участие почти 300 тысяч молодых людей в возрасте от 11 до 17 лет.

Организация UK Cyber Cluster Collaboration содействует установлению партнерских связей между отраслью, школами и колледжами, чтобы обеспечить доступ к возможностям и знаниям во всех регионах.

Программа NCA Cyber Choices направлена на повышение осведомленности молодых людей и обеспечения их доступа к таким альтернативам, как ученичество и стажировка, помогая им принимать обоснованные решения и использовать свои кибернавыки, не нарушая закона

[25] Правительство Соединенного Королевства, Cyber security skillls in the UK labour market (2021)

Основополагающая цель 2: киберустой-чивость

Построение в Соединенном Королевстве устойчивой и процветающей цифровой экономики

87. Кибербезопасность и киберустойчивость имеют фундаментальное значение для достижения нами, как кибердержавой, наших стратегических целей в целом: не обеспечив кибербезопасность и киберустойчивость, мы не сможем использовать все преимущества преобразующего потенциала цифровых технологий, чтобы восстановить всё лучше, справедливее и прочнее, чем было, и защитить британское стратегическое преимущество в киберпространстве и с его помощью. Мы должны продолжать формирование прочной киберзащиты, принимая меры для укрепления безопасности британских цифровых сетей, информации и активов на национальном, местном и индивидуальном уровнях, а также повышать их устойчивость на случай возникновения инцидентов.

88. В этом разделе мы сосредоточим внимание на киберустойчивости, которая будет в полной мере эффективной только в том случае, если станет частью общей, основанной на усилиях всего общества деятельности, по укреплению британской киберустойчивости. В готовящейся Стратегии национальной устойчивости — подготовка которой является одним из ключевых обязательств в рамках Интегрированного обзора — будет изложен общий подход к национальной устойчивости.

89. За последнее десятилетие был достигнут значительный прогресс в укреплении киберустойчивости — образован Национальный центр кибербезопасности (NCSC), повышена доступность к рекомендациям, руководствам и другим инструментам и введены в действие законы, в том числе Положения о сетях и информационных системах («Положения NIS») и Общий регламент по защите данных и Закон 2018 года о защите данных. Однако серьезные пробелы остаются. Нарушения кибербезопасности сказываются на работе правительства, компаний, организаций и граждан; многие организации все еще сообщают о большом числе нарушений кибербезопасности или атак.

90. Опираясь на основы, заложенные предыдущей стратегией, мы будем совершенствовать наш подход и сместим акцент в сторону киберустойчивости Соединенного Королевства, обращая особое внимание на следующие аспекты:

- наращивание усилий, направленных на обеспечение автоматического повышения безопасности интернета, предотвращение атак и разработку мер базовой защиты на благо всех британских компаний, организаций и граждан, а также активизация поддержки, доступной для лиц, наименее способных защитить себя в интернете;
- постановка перед правительством задачи на собственном примере демонстрировать внедрение передовой практики в области кибербезопасности;
- интеграция кибербезопасности в качестве одной из главных составляющих эффективного бизнеса путем оптимизации применения регулятивных мер и других стимулов, а также использование аналитических данных об угрозах для создания сообществ, способных защищать себя;

- подведение фундамента под эти меры с использованием поддающихся объективному измерению стандартов, фактов и данных и переход от сбора данных к использованию их для принятия мер.

91. В данной стратегии концепция киберустойчивости имеет три основных аспекта. Первый — необходимость понимания характера **рисков**. Второй — необходимость принимать меры **безопасности** для предотвращения и сдерживания кибератак. Третий — учитывая возможность атак, необходимость готовиться к ним, обеспечивать **устойчивость** на достаточно высоком уровне, чтобы сводить их воздействие к минимуму и повысить способность к восстановлению.

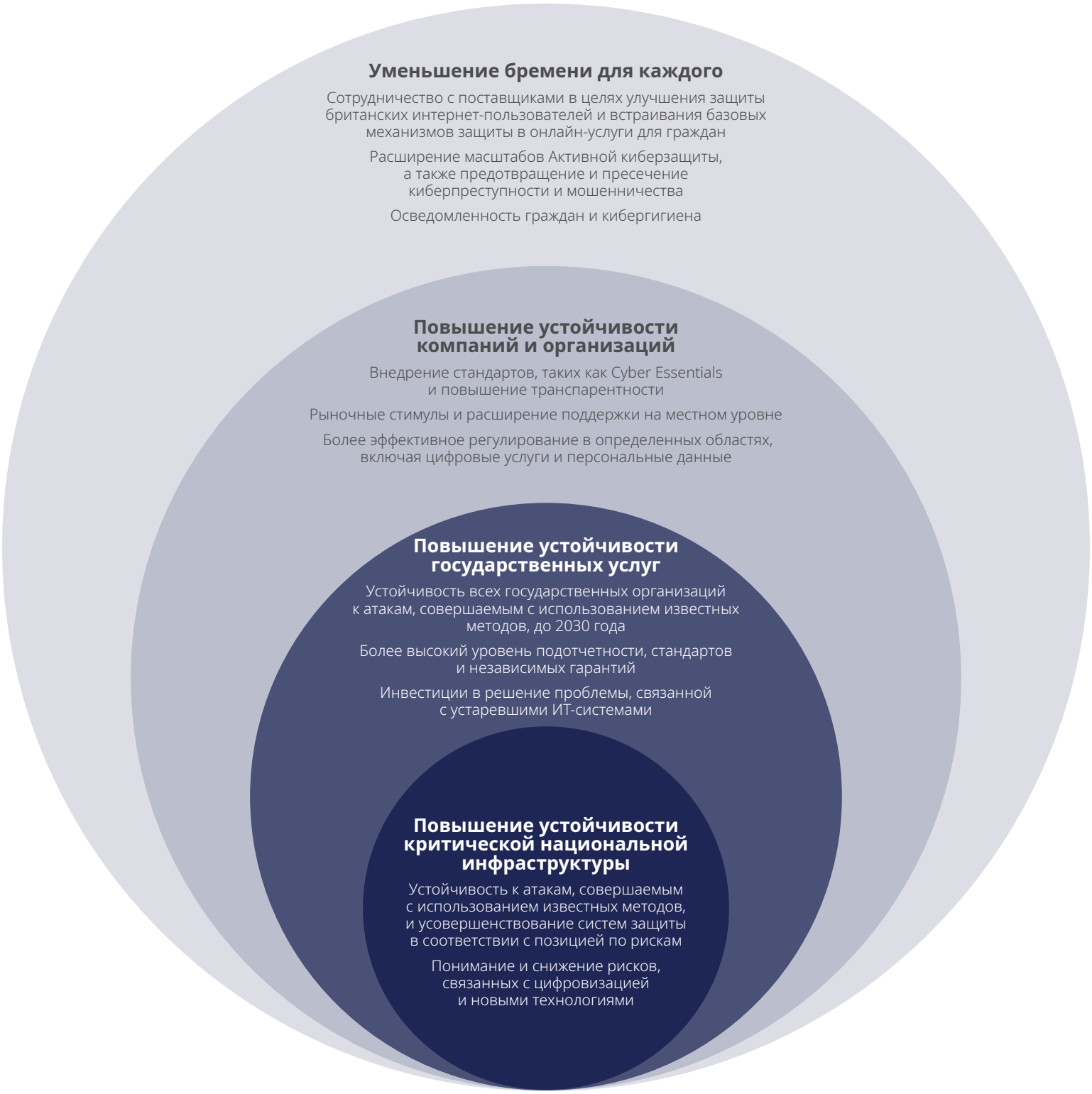
92. Наш подход, опирающийся на национальные возможности реагирования на системные риски, будет адаптирован с учетом особенностей каждой аудитории. Аудитории, которые мы стремимся включить в сферу нашей защиты и влияния, — это британские граждане, компании и организации, правительство и государственный сектор, а также те, кто управляет нашей критической национальной инфраструктурой (обеспечивая предоставление ключевых услуг в таких областях, как поставка питьевой воды, электроэнергетика, финансы, транспорт и электросвязь, от которых зависим мы все).

93. Мы сосредоточим усилия, в первую очередь, на мерах по обеспечению безопасности цифровой среды для всех британских пользователей интернета, предотвращению атак, укреплению базовой безопасности продуктов и услуг и содействию гражданам, предприятиям малого бизнеса и организациям в принятии основных мер для повышения кибербезопасности. Далее — взаимодействие с теми, кто несет большую ответственность и имеет возможности для осуществления дополнительных, соразмерных риску мер по укреплению безопасности и устойчивости: в конечном итоге это обеспечит высочайший уровень защиты основных государственных и жизненно важных услуг, от которых зависят наш народ и наша экономика.

94. Это потребует совместных усилий государства, всех секторов экономики и общества. Обязанность правлений компаний и организаций — управлять своими киберрисками. Наша цель — определить четкие ожидания, основанные на надлежащей системе стимулов, мерах поддержки и регулирования, способствующие достижению улучшений и переносу бремени управления рисками кибербезопасности с конечных пользователей на тех, кто лучше всего способен справляться с ними.

95. Мы требуем, чтобы государственные ведомства, государственный сектор в целом и регулируемые операторы критической национальной инфраструктуры (КНИ) повысили свои стандарты и обеспечили более проактивное управление своими рисками. Мы ожидаем повышения ответственности крупных компаний и организаций, включая поставщиков цифровых услуг и платформ, за обеспечение защиты своих систем, услуг и клиентов в рамках своей основной деятельности. Со своей стороны правительство будет прилагать больше усилий к укреплению безопасности цифровой среды и реагированию на системные риски, а также оказывать помощь путем предоставления рекомендаций и инструментов, а также содействия аккредитации на рынке и развитию навыков, позволяющих достигать улучшений.

96. Наши усилия, направленные на повышение киберустойчивости в Соединенном Королевстве, также должны быть неотъемлемой частью нашей международной деятельности. Углубление глобализации цепочек поставок, ИТ-платформ, многонациональных компаний и самого интернета означает, что в одиночку мы не сможем повысить кибербезопасность Соединенного Королевства. В ответ на этот вызов мы должны и далее углублять понимание связей между кибербезопасностью Соединенного Королевства и глобальной кибербезопасностью, принимать меры в областях высокого риска и совместно с международными партнерами работать над укреплением устойчивости, которая создает благоприятные условия для цифрового преобразования, безопасности и торговли, отвечающих общим интересам, как изложено в главе об Основополагающей цели 4 «Глобальное лидерство».


Уменьшение бремени для каждого
Сотрудничество с поставщиками в целях улучшения защиты британских интернет-пользователей и встраивания базовых механизмов защиты в онлайн-услуги для граждан
Расширение масштабов Активной киберзащиты, а также предотвращение и пресечение киберпреступности и мошенничества
Осведомленность граждан и кибергигиена
Повышение устойчивости компаний и организаций
Внедрение стандартов, таких как Cyber Essentials и повышение транспарентности
Рыночные стимулы и расширение поддержки на местном уровне
Более эффективное регулирование в определенных областях, включая цифровые услуги и персональные данные
Повышение устойчивости государственных услуг
Устойчивость всех государственных организаций к атакам, совершаемым с использованием известных методов, до 2030 года
Более высокий уровень подотчетности, стандартов и независимых гарантий
Инвестиции в решение проблемы, связанной с устаревшими ИТ-системами
Повышение устойчивости критической национальной инфраструктуры
Устойчивость к атакам, совершаемым с использованием известных методов, и усовершенствование систем защиты в соответствии с позицией по рискам
Понимание и снижение рисков, связанных с цифровизацией и новыми технологиями

Задача 1. Улучшить понимание киберрисков, чтобы повысить эффективность мер кибербезопасности и киберустойчивости.

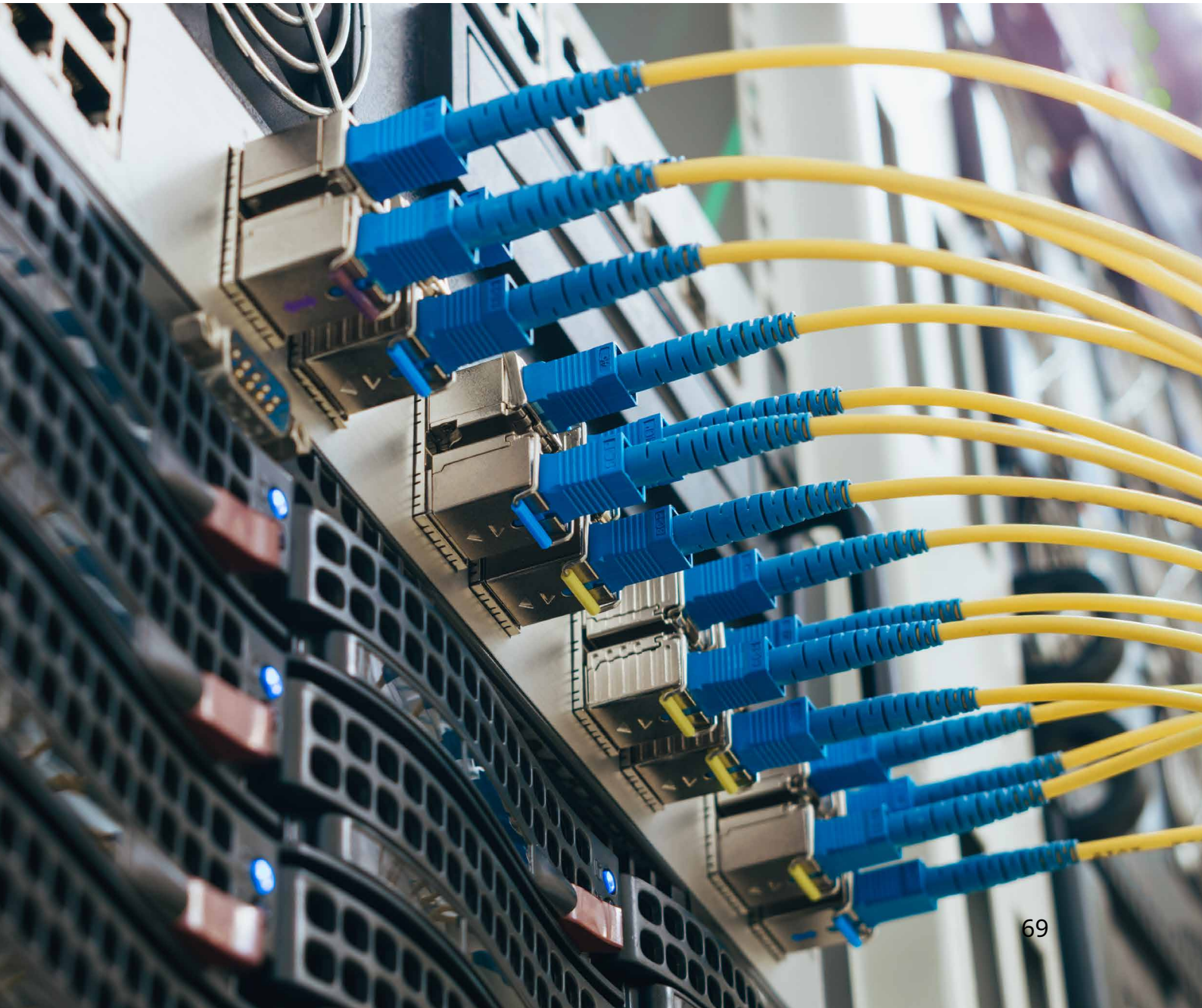
97. Мы обеспечим как можно более тесное сотрудничество между правительством, компаниями и организациями, чтобы улучшить коллективное понимание рисков, правильно расставить приоритеты и обосновать необходимость действий. Мы будем оказывать поддержку гражданам в сотрудничестве с компаниями и организациями, которые предоставляют услуги потребителям, а также далее укреплять способность государства к выявлению сквозных рисков. К 2025 году мы достигнем следующих результатов:

98. Правительство будет иметь актуальное стратегическое понимание киберрисков, стоящих перед страной, и, опираясь на него, выявлять системные риски, распространять информацию о приоритетах, а также содействовать проведению в жизнь стратегии и достижению результатов. Мы будем способствовать сохранению и получению дальнейших выгод от крупных инвестиций, вложенных в «понимание угроз» в соответствии с предыдущей Национальной стратегией кибербезопасности, и расширять уже предпринимаемые усилия, направленные на улучшение понимания рисков во все более взаимосвязанном мире. Сюда входит определение областей, в которых концентрация цифровых цепочек поставок стала слишком высокой, и сотрудничество с международными партнерами в сфере управления коллективными рисками. Мы также оптимизируем регистрацию данных о нарушениях Закона о неправомерном использовании компьютерных технологий (CMA), чтобы лучше понимать связи между нарушениями безопасности данных и преступлениями, к которым они ведут, а также углубить знания о том, как преступления, предусмотренные законом CMA, способствуют осуществлению других видов преступлений.

99. Правительство на собственном примере демонстрирует важность понимания киберрисков. Мы будем применять разработанный NCSC Механизм оценки киберрисков (CAF) в качестве системы обеспечения качества во всех государственных ведомствах, а также определим связи между критически важными системами и общими поставщиками. Мы создадим новый Правительственный координационный центр кибербезопасности (GCCC) и межведомственную Службу уведомлений об уязвимостях (VRS), которые позволят правительству обеспечить «единую оборону» в ходе управления инцидентами, уязвимостями и угрозами. Служба VRS будет поддерживать полезные и доверительные отношения с научно-исследовательскими организациями, работающими в области безопасности, обеспечивая снижение уязвимости в масштабе всех государственных активов. Мы будем и далее поддерживать и координировать работу с аналогичными службами в автономных правительствах, такими как центральное координирующее подразделение по киберустойчивости, которое планируется создать в Шотландии.

100. У нас будет более глубокое понимание киберрисков в масштабах всей КНИ Соединенного Королевства. Мы будем способствовать более широкому применению Механизма оценки киберрисков (CAF) или эквивалентных систем в масштабах всех секторов КНИ и повысим совместимость с другими механизмами оценки кибербезопасности и отчетности, которые уже используются. Мы проведем обзоры критичности объектов и составим карту зависимостей в рамках КНИ и ее цепочек поставок. Мы укрепим партнерские связи с владельцами и операторами КНИ, чтобы улучшить доступ к информации об угрозах и рисках и согласовать позицию по рискам. Мы будем стремиться к пониманию новых рисков и областей, в которых в результате цифровизации и внедрения новых технологий появляются новые объекты КНИ, в том числе в рамках более широких приоритетов, таких как переход к чистому нулевому уровню выбросов.

101. Британские компании и организации лучше понимают киберриски и свою ответственность за управление ими. Мы будем помогать организациям лучше понять риски, стоящие перед их клиентами, в частности то, как данные, которые у них хранятся, могут быть использованы для совершения преступлений, таких как мошенничество, кража личности или вымогательство. И мы будем предоставлять больше аналитических данных, полученных в ходе исследований, а также информацию о распространенности и воздействии кибератак и об относительном прогрессе в повышении кибербезопасности, достигнутом в секторах.



Задача 2. Повысить эффективность предотвращения и сдерживания кибератак путем оптимизации управления киберрисками в британских организациях и улучшения защиты граждан.

102. Наш подход к предотвращению и сдерживанию кибератак предполагает что: (i) организации должны отвечать за принятие мер по управлению своими киберрисками, однако, чтобы это стало приоритетом, требуется укрепление структур подотчетности и эффективное управление на уровне правления; (ii) в рамках сотрудничества с отраслью роль правительства должна заключаться в принятии непосредственных мер, направленных на масштабное снижение рисков, если у него для этого есть уникальные возможности, и (iii) мы должны предоставлять поддержку и рекомендации гражданам, индивидуальным предпринимателям, малым предприятиям и организациям, чтобы помочь им управлять собственными рисками. К 2025 году мы достигнем следующих результатов:

103. Правительство добилось масштабного снижения ущерба, наносимого Соединенному Королевству, и уменьшения бремени для британских граждан. Мы будем активнее принимать упреждающие меры в интересах всех интернет-пользователей в Соединенном Королевстве, расширяя деятельность в рамках Активной киберзащиты, направленную на поддержку более широкого ряда секторов, включая благотворительные и научные организации, малые и средние предприятия и граждан. Мы также усилим механизмы защиты онлайновых сервисов путем активизации взаимодействия и обмена информацией с отраслью.

104. Эта деятельность дополняет работу над другими приоритетами правительства, направленную на защиту граждан Соединенного Королевства в интернете, такую как разработка проекта Закона о безопасном интернете и политики противодействия экономическим преступлениям, таким как мошенничество.

105. Это потребует более тесного сотрудничества с соответствующими секторами, включая поставку онлайновых сервисов, электросвязь, технологии, банковскую сферу и розничную торговлю, в целях улучшения защиты британских интернет-пользователей, включая усложнение регистрации вебсайтов для незаконных целей, более эффективное удаление и блокирование вредоносного контента в интернете, повышение способности к восстановлению и возвращению похищенных регистрационных данных и повышение безопасности британской телекоммуникационной инфраструктуры. Мы также разработаем варианты законодательного обеспечения защиты граждан, если принятия мер на добровольной основе окажется недостаточным.

106. Наши усилия по масштабному снижению ущерба также предусматривают снижение системных рисков, связанных с цифровыми цепочками поставок. При необходимости мы будем принимать меры вмешательства в целях диверсификации цепочек поставок, так как мы это делаем в секторе электросвязи; мы будем укреплять нашу коллективную экономическую безопасность за счет более эффективного обмена информацией и применения надежных, прогнозируемых и соразмерных подходов к скринингу прямых иностранных инвестиций (ПИИ) в критически важные сектора и разработаем четкие требования к критически важным и общим поставщикам продуктов и услуг государству.

107. Значительно повышена устойчивость государственной критической инфраструктуры к кибератакам, и все правительственные организации — в масштабах всего государственного сектора — будут устойчивыми к известным уязвимостям и видам атак к 2030 году. Наша цель — сделать британский государственный сектор образцом в области применения наилучшей практики. В этой связи мы опубликуем первую специальную Стратегию кибербезопасности правительства. Она будет сосредоточена на более эффективных процессах управления рисками, надлежащем управлении и подотчетности; централизованной разработке и внедрении средств и возможностей (в том числе в рамках Активной киберзащиты); более комплексном мониторинге систем, сетей и услуг; оперативном

и масштабном реагировании на инциденты и на инвестициях в квалифицированные кадры, знания и культуру, поощряющие устойчивые перемены.

108. Осуществляется более эффективное управление киберрисками для критической национальной инфраструктуры Соединенного Королевства. Такие услуги по определению являются наиболее критически важными для страны. Мы продолжим тесно сотрудничать с операторами, чтобы как можно быстрее обеспечить устойчивость к атакам, осуществляемым распространенными методами, и ввести в действие более совершенные механизмы защиты, где это целесообразно. Для операторов жизненно важных услуг, указанных в Положениях NIS, это означает необходимость как минимум обеспечить базовые стандарты, установленные соответствующими компетентными органами для каждого сектора.

109. В этой связи мы сделаем обзор возможностей правительства в плане привлечения операторов КНИ к ответственности, чтобы обеспечить вкладывание ими средств в повышение кибербезопасности критически важных систем и эффективное управление рисками, в том числе связанными с цепочками поставок. Мы укрепим нормативную базу, чтобы расширить ее охват, действенность и способность к адаптации в контексте рисков для национальной безопасности в целом и стремительного изменения характера угроз и технологий. Мы начнем с консультаций по вопросам реформирования Положений NIS, внедрения нового механизма безопасности для британских поставщиков услуг электросвязи и разработки соответствующей нормативной базы, чтобы обеспечить безопасность и устойчивость будущих британских интеллектуальных и гибких энергосистем, необходимых для достижения чистого нулевого уровня, к киберугрозам.

110. Наряду с этим мы будем: расширять возможности регулирующих органов; инвестировать в подготовку квалифицированных кадров, чтобы дать возможность операторам КНИ привлекать, развивать и удерживать киберспециалистов (см. главу о Британской кибернетической экосистеме); и помогать операторам управлять рисками для цепочек поставок путем активизации взаимодействия с поставщиками критических услуг и использования всех рычагов влияния — от рекомендаций до предложений, связанных с вопросами законодательства и поставок.

111. Инфраструктура, поддерживающая использование нами данных, является защищенной и устойчивой. Инфраструктура — жизненно важный национальный актив, который поддерживает нашу экономику, обеспечивает предоставление государственных услуг и содействует росту. Мы будем играть более важную роль в обеспечении надлежащей защиты данных в процессе их обработки, передачи и хранения в больших объемах, например во внешних центрах данных. Мы создадим более прочный механизм управления рисками, чтобы повысить стандарты безопасности и устойчивости в масштабах всего сектора, и осуществим положения Закона о национальной безопасности и инвестициях 2021 года, чтобы укрепить систему скрининга инвестиций. Мы укрепим сотрудничество с международными партнерами, обеспечивая, чтобы расширение доступа к глобальным данным и потокам данных не повышало рисков для безопасности Соединенного Королевства, а также примем меры для решения проблем безопасности, связанных с массовым сбором данных.

112. Мы также будем принимать во внимание повышение критического значения британских инфраструктурных услуг в области обработки данных для поддержки экономики и их роли в системе критической национальной инфраструктуры. Эти меры осуществляются в соответствии с обязательствами, изложенными в Национальной стратегии в области данных и Интегрированном обзоре.

113. Все больше британских компаний и организаций проактивно управляют своими рисками и принимают меры для повышения своей киберустойчивости. Мы будем оказывать поддержку и содействовать поведенческим изменениям путем разработки рыночных стимулов для поощрения эффективной киберзащиты. По необходимости мы дополним это специальным законодательством, призванным обеспечить эффективное управление киберрисками теми, кто несет за это наибольшую ответственность, а также сохранение действенности британского законодательства в области кибербезопасности в свете эволюционирующих угроз и технологий.

114. В этой связи мы активизируем сотрудничество с влиятельными рыночными игроками (закупщиками, финансовыми учреждениями, инвесторами, аудиторами и страховщиками), чтобы создать стимулы для применения надлежащих мер кибербезопасности в масштабах всей экономики. Мы внесем предложения по оптимизации корпоративной отчетности об обеспечении устойчивости к рискам, включая киберриски. Это позволит инвесторам и держателям акций лучше понять, как компании управляют материальными рисками для своего бизнеса и обеспечивают их снижение. Мы будем и далее поощрять участие компаний в программах аккредитации и стандартизации, таких как программа сертификации Cyber Essentials, а также участие их правлений в управлении киберрисками.

115. Специальное законодательство, прежде всего, будет сосредоточено на секторах, кибератака на которые потенциально может иметь самые серьезные последствия, в том числе на поставщиках некоторых критически важных и цифровых услуг, а также на защите данных в масштабах экономики в целом и в крупных компаниях в частности. Оно дополнит План цифрового регулирования и на начальном этапе будет сосредоточено на положениях, регулирующих обеспечение безопасности сетей и информационных систем (NIS), как описано выше и в разделе о технологиях, и на последующих шагах по реформированию британского режима защиты персональных данных.

116. Дополнительная информация о мерах, которые мы предпримем для повышения устойчивости бизнеса и киберустойчивости в масштабе всех британских компании и организаций, будет включена в Обзор мер регулирования и стимулирования в области кибербезопасности.

117. Технические рекомендации, инструменты самопомощи, а также продукты и услуги гарантированного качества, предназначенные для повышения киберустойчивости, легко доступны и постоянно совершенствуются, при этом особое внимание уделяется помощи гражданам, индивидуальным предприятиям и небольшим организациям. Мы продолжим разрабатывать технически корректные, своевременные и практически выполнимые рекомендации и инструменты самопомощи силами NCSC. Мы будем обеспечивать согласованность и точность информации, передаваемой по самым эффективным каналам, будь то кампания Cyber Aware, вебсайт NCSC, правительственные структуры, правоохранительные сети или партнерства с отраслью; а также расширим доступ к поддержке на местном уровне. В рамках программы Digital Entitlement мы продолжим финансировать получение взрослыми гражданами необходимой квалификации в области базовых навыков работы с цифровыми технологиями, чтобы они имели нужные навыки для обеспечения безопасности и ответственного поведения в интернете. Кроме того, мы будем помогать компаниям и организациям ориентироваться на сложном рынке кибербезопасности, расширяя механизмы гарантии качества продуктов и услуг и разрабатывая коммерческие предложения в рамках сертификации Cyber Essentials, которые облегчат доступ предприятий малого бизнеса к базовым рекомендациям.

Элис Пауэр, сотрудник по вопросам киберзащиты и предотвращения кибератак, региональное подразделение по борьбе с киберпреступностью TARIAN

Региональное подразделение по борьбе с киберпреступностью TARIAN — мультидисциплинарная команда служащих полиции и персонала, прикомандированных от Службы полиции Уэльса. Их миссия — содействовать созданию более защищенной и безопасной киберсреды в Южном Уэльсе.

Элис Пауэр, сотрудник по вопросам киберзащиты и предотвращения кибератак, работает в группе по взаимодействию:

«Это клише, но в нашем подразделение не бывает «типичных» дней. Сегодня я могу отвечать за подготовку презентаций с рекомендациями для внутренних полицейских ведомств или внешних организаций, чтобы дать им четкое понимание того, как они могут защитить себя и свою рабочую среду от киберугроз. А завтра я могу выступать с презентацией перед школьниками по широкому спектру тем — от интернет-безопасности до Закона 1990 года о неправомерном использовании компьютерных технологий. Я часто принимаю участие во встречах с партнерскими агентствами и службами, чтобы обсудить новые угрозы и соответствующие руководства для наших аудиторий. Я также осуществляю взаимодействие с организациями, от которых мы получаем сообщения об уязвимостях, принимаю участие в национальных операциях, а также выступаю в качестве гостя на разных мероприятиях и конференциях и нахожу время для постоянного совершенствования своих навыков, способностей и знаний».

Задача 3. Повышать устойчивость на национальном и организационном уровнях, чтобы быть готовыми к реагированию на кибератаки и восстановлению после них.

118. Несмотря на усилия, направленные на понимание рисков, и принятие превентивных мер, инциденты все еще случаются. Мы должны укреплять возможности для управления инцидентами и реагирования на них во всех организациях, чтобы свести к минимуму ущерб и оказывать более действенную поддержку жертвам. К 2025 году мы достигнем следующих результатов:

119. Британское стратегическое управление и координация мер реагирования на киберинциденты национальной значимости будут еще более эффективными. Мы будем опираться на накопленный правительством опыт реагирования на крупные киберинциденты, используя извлеченные уроки, чтобы усовершенствовать наши политики и процессы. Мы будем передавать опыт урегулирования кризисов международным партнерам и отраслевым предприятиям, и, в свою очередь, определять примеры передового опыта, накопленного другими, чтобы повышать свою готовность и совершенствовать процессы. Мы обеспечим, чтобы у групп реагирования на инциденты в составе NCSC и правоохранительных органов, были необходимые знания и инструменты для реагирования на весь спектр постоянно меняющихся видов инцидентов и для координации национальных мер реагирования на приоритетные угрозы.

120. Упростилась процедура сообщения о киберинцидентах, и поддержка жертвам киберпреступлений стала более эффективной. Сообщаемая информация также поможет предотвращать будущие инциденты и будет использоваться правоохранительными органами при осуществлении деятельности по расследованию и пресечению киберпреступлений и уголовному преследованию преступников. В этой связи мы создадим новую национальную службу регистрации и анализа мошенничества и киберпреступлений, которая заменит собой Action Fraud к 2025 году. Мы будем поощрять другие способы уведомления о киберинцидентах, в том числе с использованием нового механизма бизнес-отчетности в Службе полиции Лондонского Сити. Мы обеспечим для регулирующих органов возможность требовать отчетность по более широкому кругу инцидентов, включая потенциально опасные происшествия, в регулируемых секторах. Образование Подразделения по работе с жертвами экономических преступлений будет способствовать улучшению поддержки и консультативной помощи, предоставляемой жертвам после стрессового и болезненного опыта.

121. Повысилась готовность правительства и КНИ к реагированию на инциденты и восстановлению после них, в том числе путем более эффективного планирования действий на случай инцидентов и регулярного проведения учений. Мы будем оказывать поддержку британскому правительству и операторам КНИ в поиске на рынке организаций, предоставляющих услуги по проведению учений и управлению инцидентами кибербезопасности, путем расширения рамок аккредитованной NCSC программы Реагирования на киберинциденты и разработки новой программы учений.

122. Будут расширены возможности мониторинга и обнаружения в правительственных ведомствах и в масштабе всех правительственных цифровых активов. Мы обеспечим изучение и использование накопленного опыта для целей повышения эффективности наших политик и процессов; будем обмениваться опытом управления кризисами с международными и отраслевыми партнерами; и обеспечивать, чтобы наши группы по управлению инцидентами имели необходимые знания, возможности и потенциал для реагирования на весь спектр постоянно совершенствующихся видов инцидентов.

123. Мы установим четкие требования в отношении проведения учений и испытаний или имитационного моделирования действий злоумышленников для всех операторов КНИ и будем стимулировать инновации и сотрудничество в области реагирования на инциденты и проведения учений с возможным применением моделей, таких как модель Координационного центра кибербезопасности финансового сектора. В рамках достижения наших амбициозных целей в технологической области (изложенных в следующей главе) мы создадим национальную лабораторию по безопасности эксплуатационных технологий в качестве центра передового опыта в области испытаний, учений и изучения критических промышленных технологий в целях наращивания соответствующего потенциала в сотрудничестве с представителями отрасли, научных кругов и международных партнеров.

124. Британские компании и организации имеют более четкое представление о том, что необходимо предпринимать в случае возникновения инцидента, к кому обращаться, кто может помочь и как восстановить деятельность. Мы улучшим доступ к программам подготовки и учений, осуществляемых с использованием отраслевых услуг гарантированного качества, в том числе новой программы Реагирования на киберинциденты и Службы организации учений по реагированию на киберинциденты. Мы будем гарантировать доступ к постоянной поддержке со стороны правоохранительных органов в масштабах всей страны для лиц, ставших жертвами киберпреступлений, и поощрять предприятия малого бизнеса и организации пользоваться услугами поддержки местных организаций, таких как региональные Центры киберустойчивости.

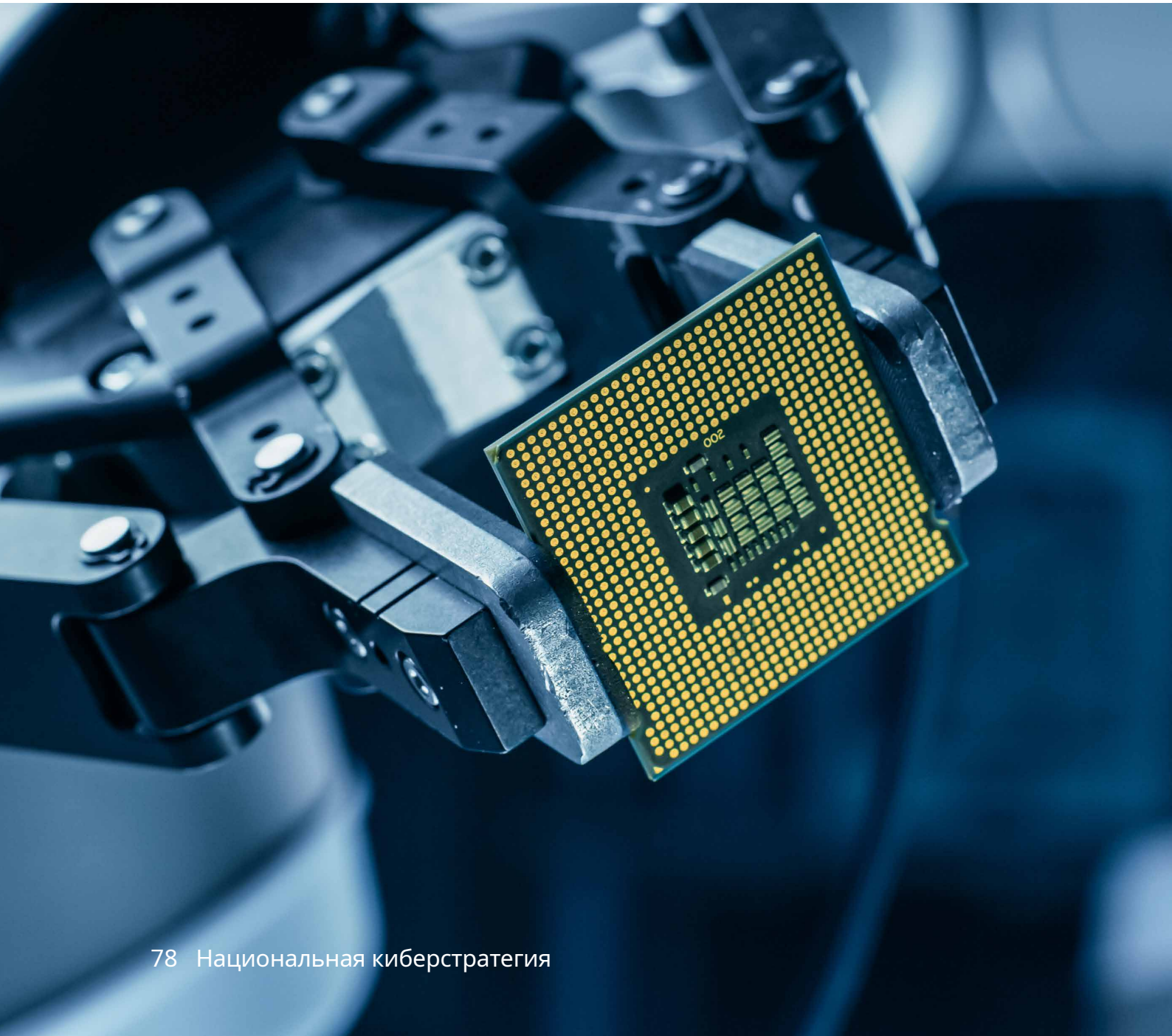
Дэниэл Ын, CEO, CyberOwl

CyberOwl пользуется преимуществами, которые обеспечивает государственная программа развития киберсектора. Мы предоставляем услуги по мониторингу и анализу кибербезопасности эксплуатационных активов в морском секторе и КНИ. Для перехода к устойчивому развитию требуется расширение возможностей подключения и цифровизации активов на местах, а это подвергает их киберрискам. CyberOwl помогает операторам определить и систематизировать свои активы, получать ранние предупреждения о киберрисках, а также убедиться в том, что они обеспечили безопасность, и продемонстрировать это регулирующим органам. Совместно с крупнейшими в мире операторами морских активов в странах EMEA и Азиатско-Тихоокеанском регионе мы обеспечиваем повышение устойчивости логистической цепочки поставок в отрасли грузоперевозок. В 2021 году мы получили в 14 раз больше заказов и вдвое увеличили масштабы нашей деятельности в Соединенном Королевстве и Сингапуре.

Джен Эллис, вице-президент по связям с сообществами и общественностью, Rapid7

В мои рабочие обязанности входит проведение разъяснительной работы со специалистами и влиятельными лицами в малых и крупных организациях и разных секторах с тем, чтобы помочь им понять, какие вызовы перед ними стоят, и найти решения для повышения их кибербезопасности. Я постоянно слышу, что организации находятся в затруднении, не зная, на чем сосредоточить усилия, с чего начать и как добиться прогресса. Кроме того, техническому персоналу бывает трудно добиться понимания и согласия руководства. Разработка правительством четкой, последовательной и транспарентной киберстратегии может помочь в решении этих проблем. Она дает техническому персоналу аргументы, которые они могут использовать в своих дискуссиях с руководством. Она укажет им, на чем следует сосредоточить усилия, а также возможные пути для выхода на более высокий уровень. Обеспечение кибербезопасности все еще остается невероятно сложной задачей, требующей непрекращающихся усилий, но широкомасштабная киберстратегия позволит улучшить понимание того, что кибербезопасность имеет большое значение, и что укрепление ее — наше общее дело.

Основополагающая цель 3: технологическое преимущество



Достижение лидерства в области технологий, жизненно важных для кибердержавы

125. Некоторые технологии имеют критическое значение для формирование будущего киберпространства. Страны, способные играть лидирующую роль в сфере этих технологий, будут иметь больше возможностей для влияния на их разработку и развертывание, и смогут лучше защищать свою безопасность, обеспечивать экономическое преимущество и оперативнее использовать возможности для совершения прорывов в разработке киберсредств. По мере того, как технологии становятся все более важным инструментом геополитического влияния, конкуренция на этой арене будет обостряться.

126. Для Соединенного Королевства получение стратегического преимущества за счет использования достижений науки и техники, а также доступа к данным, от которых оно зависит, является необходимым условием для достижения своих целей как кибердержавы в целом. При осуществлении предыдущих стратегий правительство предприняло шаги для стимулирования исследований и инноваций в области технологий кибербезопасности, например, в рамках программ акселерации стартапов и деятельности Центров передового опыта в области исследований кибербезопасности, а также поощряло разработку потребительских устройств, «безопасных по дизайну». Однако сейчас нам требуется более амбициозный и проактивный подход, позволяющий сохранить ведущие позиции в области критических технологий и избежать чрезмерной зависимости от конкурентов и противников.

127. В Интегрированном обзоре изложены планы по закреплению за Соединенным Королевством статуса научно-технической супердержавы и использованию достижений науки и техники для получения и сохранения стратегического преимущества. Настоящая стратегия предусматривает поддержку деятельности Национального совета по науке и технике и Управления по работе над Стратегией развития науки и техники, направленной на достижении этой цели и дополняющей британские стратегии в таких областях, как искусственный интеллект, квантовые технологии и данные.

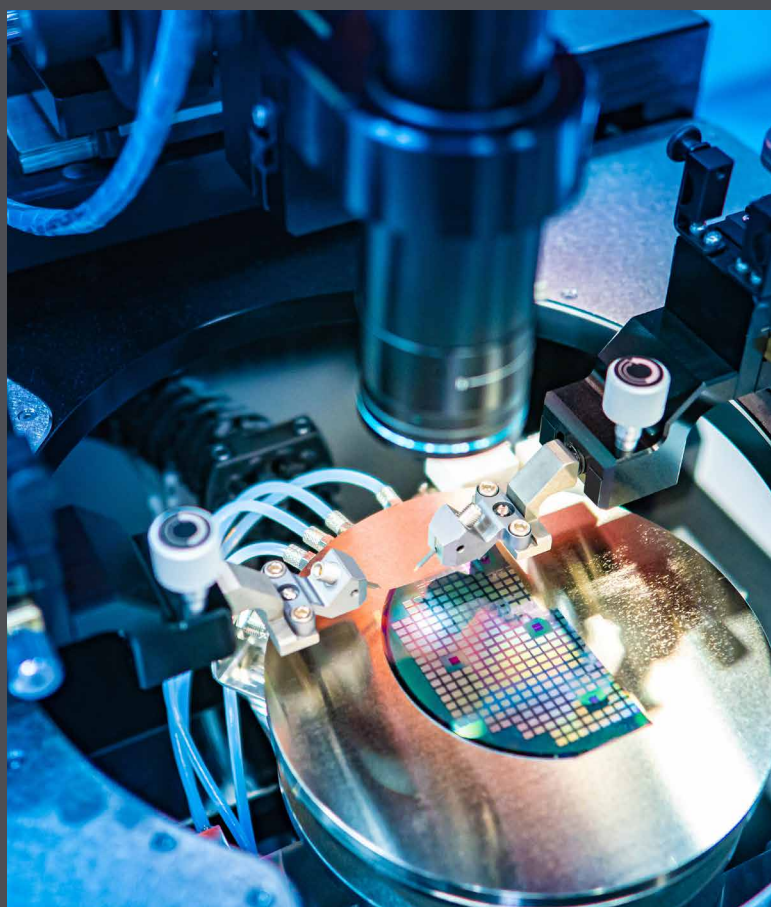
128. Опираясь на технический опыт и знания Национального центра кибербезопасности (NCSC) и других правительственных организаций, мы укрепим нашу способность определять технологические области, имеющие критическое значение для сохранения нашей кибермощи. Мы будем принимать стратегические решения о приоритетах на национальном уровне, используя модель «владеть-сотрудничать-приобретать», описанную в Интегрированном обзоре. В отдельных областях мы будем вкладывать средства в научно-исследовательскую деятельность и в стратегические партнерства, необходимые для наращивания внутреннего потенциала Соединенного Королевства. Кроме того, в областях с высокой зависимостью от глобальных рынков мы, совместно с отраслевыми предприятиями, регулирующими органами и международными партнерами, будем содействовать созданию надежных и диверсифицированных цепочек поставок и устанавливать стандарты, обеспечивающие безопасность и открытость технологий. Мы также будем укреплять способность Соединенного Королевства к использованию и защите растущих объемов данных и информации, генерируемых в результате развития новых технологий и стимулирующих инновации в них, при помощи механизмов, описанных в Национальной стратегии в области данных, чтобы обеспечить максимальные преимущества для нашей экономики и общества.

Технологии, жизненно важные для сохранения кибермощи

Разнообразие существующих и новых технологий будет иметь критическое значение для сохранения кибермощи Соединенного Королевства. Мы также должны уметь предвосхищать, оценивать и использовать эти достижения. В процессе осуществления стратегии мы планируем уделять приоритетное внимание ряду технологий и сфер применения, описанных ниже. Это не исчерпывающий или статичный перечень, и мы, в сотрудничестве с предприятиями отрасли, научными кругами и техническими экспертами, будем и далее уточнять наши приоритеты:

- технологии 5G и 6G и другие новые формы передачи данных;
- искусственный интеллект (ИИ), в том числе необходимость защиты ИИ-систем, и возможность использования ИИ для укрепления кибербезопасности в разнообразных сферах применения, таких как мониторинг сетей;
- технология блокчейн и сферы ее применения, такие как криптовалюта и децентрализованные финансы;
- полупроводники, микропроцессорные кристаллы, микропроцессорная архитектура и соответствующие цепочки поставок, проектирование и производственный процесс;
- криптографическая аутентификация, включая авторизацию, управление доступом и криптографические продукты высокой надежности;
- Интернет вещей и технологии, используемые в потребительской, корпоративной, промышленной и физической средах, таких как «умные города»;
- квантовые технологии, в том числе квантовые вычисления, квантовые датчики и постквантовая криптография.

Эта деятельность будет содействовать реализации целого ряда стратегий и результатов — и осуществляться в согласовании с ними — в масштабах всего правительства. Среди них — Национальная стратегия в области данных, Национальная стратегия в области ИИ и Интегрированный обзор, а также результаты, ориентированные на развитие технологий, в рамках этой Цели.



Задача 1: повысить нашу способность предвосхищать, оценивать и использовать достижения науки и техники, имеющие жизненно важное значение для нашей кибермощи.

129. Чтобы получить и сохранить конкурентное преимущество в области кибертехнологий, нам требуется скоординированный, строгий и последовательный подход к определению и анализу критически важных областей науки и техники и установлению приоритетных направлений для приложения усилий на национальном уровне. Для этого потребуется дальнейшее наращивание исследовательского и технического потенциала в правительстве и научных организациях. Мы объединим его с новыми государственными структурами, занимающимися сканированием горизонтов в области науки и техники и сбором оперативной информации, а также будем использовать наработки отраслевых экспертов и возможности наших зарубежных сетей для углубления понимания приоритетов и систем международных партнеров и конкурентов. К 2025 году мы достигнем следующих результатов:

130. Улучшились возможности правительства для выполнения анализа новых и перспективных областей науки и техники и понимание их воздействия на британскую политику и стратегию в области кибербезопасности. Мы будем расширять наши исследовательские возможности, в том числе за счет создания нового центра прикладных исследований NCSC в Манчестере, ориентированного на развитие нарождающихся технологий в таких областях как «умные города» и транспорт, который будет работать наряду с экспертами из Государственного управления по делам науки и других организаций. Мы будем обращаться к знаниям, накопленным за пределами правительства, поддерживать деятельность четырех Институтов исследований кибербезопасности и девятнадцати Центров передового академического опыта в области кибербезопасности, финансировать присуждение наград Pathfinder Awards исследователям в приоритетных областях и более эффективно использовать наше присутствие за рубежом и связи с международными партнерами.

131. Более глубокое понимание способствует более оперативному и эффективному использованию этих знаний в общей деятельности правительства по сканированию горизонтов, установлению приоритетов и принятию решений, позволяя нам применять более проактивный подход к использованию возможностей и снижению рисков. Мы образуем новое внутреннее подразделение по сканированию горизонтов, чтобы иметь возможность предвосхищать прорывы в науке и техники и понимать их значение для киберсектора. Мы будем принимать более обоснованные решения по определению приоритетов в области ключевых кибертехнологий, выбирая те направления НИОКР и разработки политики, которые обеспечивают преимущества в контексте безопасности Соединенного Королевства. Если это целесообразно, они будут использоваться Управлением по работе над Стратегией развития науки и техники и Национальным советом по науке и технике для принятия обоснованных решений при определении приоритетов в области науки и техники в целом.

Майре О'Нилл, главный следователь в Центре безопасных информационных технологий (CSIT)

CSIT — один из ведущих британских университетских центров, занимающихся исследованиями в области кибербезопасности. Этот центр, которым руководит главный следователь профессор Майре О'Нилл, одним из первых в стране получил статус центра инноваций и знаний в 2009 году. Успехи CSIT в области исследований, инноваций и взаимодействия с отраслью, достигнутые за последнее десятилетие, значительно укрепили его репутацию, как на национальном, так и на международном уровне. Деятельность CSIT, направленная на поддержку отделившимся подразделениям, расширение местного бизнеса и ПИИ в этом регионе, была одним из решающих факторов, обеспечившим успех Кластера кибербезопасности Северной Ирландии. Стартовав с нуля в 2009 году, киберсектор Северной Ирландии сейчас насчитывает 2300 сотрудников в 104 компаниях, генерируя заработную плату в размере 110 млн фунтов стерлингов ежегодно.

Задача 2. Наращивать и сохранять суверенные и союзнические преимущества в области безопасности технологий, имеющих критическое значение для киберпространства.

132. Там, где Соединенное Королевство обладает потенциалом для выхода на ведущие позиции или получения конкурентного преимущества в ключевых областях кибертехнологий, или там, где зависимость от источников поставок, которые находятся в странах, не являющихся союзниками, создает неприемлемые риски для безопасности, мы будем стремиться к развитию собственной промышленной базы. В некоторых областях нам может понадобиться сохранить по-настоящему суверенный потенциал, тогда как в других мы можем сотрудничать с международными партнерами или стремиться к выходу на лидирующие позиции в одном из сегментов рынка. Для этого потребуется скоординированный подход к стимулированию инноваций и НИОКР в сотрудничестве с отраслью и научными кругами. К 2025 году мы достигнем следующих результатов:

133. Соединенное Королевство преуспело в трансляции результатов исследований в инновации и создании новых компаний в областях технологий, имеющих жизненно важное значение для укрепления нашей кибермощи. Мы будем оказывать поддержку ученым по всему Соединенному Королевству в коммерческой разработке и внедрению в практику решений, основанных на результатах их исследований, путем применения к сотрудничеству с отраслевыми партнерами подхода, ориентированного на преодоление вызовов. Это позволит определять идеи, обладающие наибольшим потенциалом, и стимулировать инвестиции со стороны финансирующих организаций. Опираясь на описанный в Стратегии инноваций подход, мы будем содействовать развитию экосистем, сложившихся вокруг ключевых технологий, и обеспечивать, чтобы британское преимущество было более прочным и труднее поддавалось копированию.

134. Соединенное Королевство упрочило свое положение мирового лидера в области надежного проектирования микропроцессоров.[26] Мы будем развивать программу «Цифровая безопасность по дизайну», в рамках которой была разработана новая, более надежная технология производства компьютерных микросхем, обеспечивающая защиту программного обеспечения от уязвимостей. Мы используем этот опыт в производстве процессоров искусственного интеллекта, чтобы дать британским поставщикам преимущество на международном уровне. Мы также будем работать вместе с участниками Национальной программы развития квантовых технологий над созданием надежной модели квантовых компьютеров и обеспечивать, чтобы британские компании были мировыми лидерами в этой области.

135. Соединенное Королевство входит в число мировых лидеров по исследованиям в области безопасности эксплуатационных технологий и критических промышленных систем управления, а также по возможностям их тестирования и практического испытания в Соединенном Королевстве. В партнерстве с промышленными предприятиями и научными организациями мы создадим национальную лабораторию по безопасности эксплуатационных технологий. Она будет служить платформой для реализации лучших в мире исследовательских программ и поставлять государственным, военным, отраслевым и международным партнерам средства, необходимые для проведения учений и испытания этих технологий в Соединенном Королевстве. И, как подчеркивается в Стратегии диверсификации цепочек поставок для телекоммуникационных сетей 5G, мы создадим Британскую лабораторию технологий электросвязи, которая объединит усилия правительства, регулирующих органов и отрасли, направленные на поддержку создания новых механизмов безопасности в электросвязи, и будет содействовать диверсификации поставщиков телекоммуникационного оборудования в британских цепочках поставок.[27]

136. Правительство способно эффективнее защищать британские инновации и интеллектуальную собственность в области критических кибертехнологий от вредоносной деятельности, обеспечивая сохранение нашего конкурентного преимущества.[28] Мы будем вкладывать средства в ресурсы и знания, необходимые для обеспечения технического руководства в области укрепления безопасности этих технологий по мере их развития, в том числе консультировать по вопросам рисков, связанных с прямыми иностранными инвестициями, в соответствии с Законом 2021 года о национальной безопасности и инвестициях. Вместе с компаниями и научными организациями мы будем и далее работать над созданием безопасной среды в ключевых областях исследований и разработок и разрабатывать эффективные меры для предотвращения хищения данных и интеллектуальной собственности.

---

[26] Микропроцессоры считаются мозгом многих устройств, которыми мы пользуемся сегодня. Они используются повсеместно, в том числе в таких критических областях, как электросвязь, оборона и здравоохранение, а также в ведущих отраслях. Технологический прогресс в области системного проектирования в настоящее время сдерживается ввиду озабоченности по поводу безопасности и защищенности, что далее усугубляется постоянным усложнением систем.

[27] Министерство цифровизации, культуры, СМИ и спорта, 5G Supply Chain Diversification Strategy (2020)

[28] С особым акцентом на сектора, обозначенные в Законе 2021 года о национальной безопасности и инвестициях, — передовая робототехника, искусственный интеллект, связь, компьютерное оборудование, криптографическая аутентификация и квантовые технологии

Цифровая безопасность по дизайну

Семьдесят процентов обнаруженных на сегодняшний день уязвимостей к киберугрозам основаны на использовании дефекта, связанного со способом проектирования микропроцессоров, и известного с 1970 года. Микропроцессоры встречаются во всех цифровых устройствах — от телевизоров до телекоммуникационного оборудования. Правительство, совместно с представителями технического сектора, работает над устранением этого дефекта, и к 2025 году появятся новые микропроцессоры для смартфонов и растущего ряда других устройств.

Для изменения дизайна микропроцессоров требуется объединение сил международных партнеров и инвестиции. Благодаря ведущим усилиям Соединенного Королевства и вложению правительством 70 миллионов фунтов стерлингов, обеспечивается интеграция безопасности в будущие устройства на этапе проектирования, что значительно снижает риск успешной кибератаки.

Эта революционная технология была исследована и разработана в Соединенном Королевстве. Технологические лидеры, включая Microsoft, Google и другие компании, вкладывают средства в реализацию этих новых преимуществ в своих продуктах, чтобы повысить их безопасность. Исследователи в университетах по всему Соединенном Королевству работают над поиском новых путей для более эффективного использования этой защищенной технологии, и правительство оказывает поддержку британским малым и средним предприятиям в поиске новых рынков для их продуктов, в которые встроена эта новая технология безопасности.

Фил Уилсон, директор по исследованиям и разработкам в The Hut Group

The Hut Group — компания, которая работает в сфере электронной коммерции и специализируется на быстро оборачиваемых потребительских товарах. У нас 200 вебсайтов, которые работают на общей платформе, обрабатывая до 3000 заказов в минуту, поэтому безопасность нашей платформы и наших клиентов имеет для нас первостепенное значение. Мы вкладываем огромные усилия в обеспечение возможностей для локализации любых кибератак, и поэтому очень рады возможности использования технического решения «Цифровая безопасность по дизайну» (DSbD) в наших системах. Использование в наших системах новых микропроцессоров, разработанных в рамках партнерской программы между правительством и отраслью с бюджетом в 180 млн фунтов стерлингов, повысит устойчивость наших систем. Однако управлять этим переходом сложно, так как мы не можем внедрять новые технологии, если они не соответствуют нашим требованиям к производительности. Нам выпала почетная возможность реализовать первый демонстрационный проект по программе DSbD, и мы надеемся в ближайшем будущем использовать преимущества этого нового решения по безопасности во всех наших системах.

Задача 2a. Сохранять эффективность и устойчивость национального центра Crypt-Key, который обеспечивает удовлетворение потребностей государственных заказчиков, наших партнеров и союзников и добился надлежащего снижения самых серьезных рисков, включая угрозы со стороны наиболее способных противников

137. Crypt-Key — термин, используемый для описания того, как Соединенное Королевство использует криптографию для защиты критической информации и услуг, от которых зависит работа британского правительства, военных ведомств и органов национальной безопасности, в том числе защита от атак со стороны наиболее способных противников. Эти возможности обеспечивают нашу способность выбирать, как мы будем развертывать свой потенциал национальной безопасности и обороны. Чтобы стать ведущей в мире страной в области разработки и применения криптографических возможностей, нам требуются квалифицированные кадры и технологии как в государственном, так и частном секторе.

138. Мы продолжим инвестировать в наращивание возможностей в правительстве и сотрудничать с британскими предприятиями, работающими в этой отрасли, обеспечивая, чтобы Соединенное Королевство оставалось одним из немногих государств, способных разрабатывать суверенные криптографические возможности в будущем. Мы также продолжим обеспечивать общее лидерство в криптографической области, в том числе оказывая поддержку НАТО в качестве одного из поставщиков материала для ключей шифрования. Это лидерство обеспечит дополнительные выгоды в плане долгосрочного развития в Соединенном Королевстве отрасли, использующей высококвалифицированную рабочую силу, и сохранения наших преимуществ в высокоустойчивой инженерии. Это будет потенциально содействовать развитию новых эффективных возможностей в других областях, требующих высокой степени надежности, таких как критическая национальная инфраструктура. К 2025 году мы достигнем следующих результатов:

139. Более жизнестойкое и защищенное британское предприятие Crypt Key с одной из самых устойчивых и лучших в мире промышленных баз, которое поставляет полный диапазон решений, необходимых Соединенному Королевству и экспортируемых некоторым партнерам и союзникам. Мы будем эффективнее объединять возможности и опыт правительства и отрасли и применять более строгий подход к управлению этим предприятием на национальном уровне. Это обеспечит наращивание базы специалистов, обладающих четко определенными специализированными навыками, которые нам необходимы.

140. Соединенное Королевство обладает более мощными криптографическими возможностями, способно реагировать на меняющиеся потребности Соединенного Королевства и его союзников и обеспечивает сохранение передовых позиций в области разработки Crypt Key. Мы обеспечим сильное техническое лидерство, чтобы углубить понимание требований пользователей и повысить качество ключевых услуг, в том числе поставку материалов для ключей шифрования и гарантирование качества продуктов и систем. Мы также преобразуем сервисы Crypt Key, сделав их более гибкими и невидимыми благодаря использованию новых технологий.

141. Соединенное Королевство укрепило свое глобальное лидерство в области Crypt Key и увеличило объем экспорта своим партнерам и союзникам. Мы сохраним ведущую роль в альянсе «Пять глаз», НАТО и других международных партнерствах и будем направлять процесс разработки международно признанных стандартов, чтобы обеспечить функциональную совместимость британских решений Crypt Key. Кроме того, мы будем работать вместе с отраслью над максимальным расширением экспортных возможностей.

Задача 3. Обеспечить безопасность новейшего поколения подключаемых технологий, снижая риски для кибербезопасности, связанные с зависимостью от мировых рынков, и обеспечивая доступ британских пользователей к надежным и разнообразным источникам поставок.

142. В течение следующего десятилетия продолжится интеграция возможностей компьютерных вычислений, подключения к интернету и автоматизации в растущее количество сегментов нашей среды, включая физические объекты и инфраструктуру и — в перспективе — самих людей. Это расширит сферу влияния киберпространства и существенно повысит объемы генерируемых данных. Способность обеспечивать безопасность и защищенность управления данными будет иметь все более критическое значение для надежного функционирования нашей экономики.

143. Мы должны обеспечить, чтобы везде, где это возможно, разработка, развитие и развертывание следующего поколения подключаемых технологий осуществлялось из расчета на безопасность и устойчивость и в рамках согласованных усилий по применению подхода, основанного на принципе «безопасности по дизайну». В силу глобальной природы цепочек поставок технологий нам понадобиться использовать все имеющиеся рычаги, чтобы более активно управлять рисками возникновения технологической зависимости.
По возможности мы будем стремиться к обеспечению встроенной безопасности; там, где это невозможно, мы будем применять строгие меры для снижения рисков, включая внутреннее регулирование и международное сотрудничество в области установления стандартов. К 2025 году мы достигнем следующих результатов:

144. Подключаемые к интернету потребительские устройства, поступающие в продажу в Соединенном Королевстве, отвечают базовым стандартам кибербезопасности.
Мы разработаем и воплотим в жизнь Законопроект о безопасности продуктов и телекоммуникационной инфраструктуры, который позволит обеспечивать соблюдение минимальных стандартов безопасности во всех новых подключаемых к интернету потребительских устройствах, поступающих в продажу в Соединенном Королевстве.
Мы поддержим кибербезопасный переход к умным и гибким энергосистемам, включая умные станции для зарядки электромобилей и умные электроприборы.
Совместно с органами по стандартизации, предприятиями отрасли и международными партнерами мы будем способствовать достижению глобального консенсуса по техническим стандартам. И мы будем помогать британским организациям повышать безопасность при осуществлении закупок и развертывании подключаемых устройств, а также управлении ими, в том числе путем подготовки нового руководства по безопасности подключаемых устройств корпоративного класса.

145. Крупные поставщики цифровых услуг, включая поставщиков облачных, программных и управляемых услуг, и магазины приложений обязаны соблюдать более высокие стандарты кибербезопасности, помогая защищать организации и потребителей от киберугроз.
Мы укрепим и расширим существующие механизмы регулирования деятельности поставщиков цифровых услуг и улучшим способность Офиса уполномоченного по информации (ICO) обеспечивать, чтобы поставщики цифровых услуг более проактивно управляли рисками, связанными с их услугами. Мы будем и далее взаимодействовать с отраслью, в том числе с крупными технологическими компаниями, в стремлении эффективно использовать рыночные знания и обеспечивать, чтобы все принимали участие в укреплении защиты британских цифровых цепочек поставок.
И мы возглавим работу по разработке международных политических решений, касающихся поставщиков цифровых услуг.

146. Соединенное Королевство идет в авангарде внедрения защищенных и устойчивых технологий «умных городов» в интересах граждан и компаний. «Умные города» обладают потенциалом для создания осязаемых преимуществ для общества — управление дорожным движением, уменьшение загрязнения, а также экономия денег и ресурсов. Однако та взаимосвязанность, которая обеспечивает более эффективное функционирование «умных городов», также создает уязвимости и возможности для кибератак. Опираясь на принятые NCSC принципы безопасности «умных городов», мы снизим риски, которым подвергаются компании, инфраструктура, государственный сектор и граждане.[29] Мы укрепим способность местных органов власти и организаций, таких как порты, университеты и больницы, закупать и использовать технологии «умных городов» безопасным способом. Мы также достигнем международного консенсуса в отношении последовательного и эффективного подхода к безопасности «умных городов».

147. Кибербезопасность встраивается в другие новые технологии, развертываемые в Соединенном Королевстве, на этапе проектирования. Мы определим сферы применения новых и нарождающихся технологий, которые создают потенциальные риски для кибербезопасности, и обеспечим, чтобы Соединенное Королевство лидировало в области надежной и защищенной разработки этих технологий. В то время, как правительство изучает возможности для развития британского потенциала в области технологии цифровых двойников и «киберфизической инфраструктуры» в целом, мы обеспечим, чтобы соображения кибербезопасности занимали центральное место при принятии решений.[30] Мы также реализуем программу гарантирования безопасности, обеспечивающую, чтобы Соединенное Королевство располагало хорошими возможностями для широкого использования целого спектра подключенных и автоматизированных транспортных средств.[31]

[29] NCSC, Connected Places Cyber Security Principles (2021)
[30] Анонсировано в Стратегии инноваций (2021)
[31] Процедура гарантирования защищенности и безопасности подключенных и автоматизированных транспортных средств (CAVPASS)

Шади А. Разак, главный технический директор и сооснователь Angoka

Публикация правительством руководства по безопасности «умных городов» и более широкое использование автономных транспортных средств подчеркивает значение безопасности в нашем обществе. Angoka — гордый выпускник программы NCSC Cyber Accelerator. Мы поставляем решения для применения в целом ряде сфер — от критической национальной инфраструктуры до технологий наземной и воздушной мобильности и многих других, обеспечивая сквозную устойчивость и гарантию безопасности.

Миссия компании — обеспечивать безопасность и устойчивость «умных городов» и технологий мобильности, которые становятся все более сложными и зависимыми от сетей подключенных устройств и межмашинного взаимодействия. Наши решения поддерживают создание доверенных зон, в которых используется децентрализованная система безопасности, устойчивая к квантовым атакам, которая динамически обновляется, постоянно представляя собой «движущуюся цель» для злоумышленников. Это означает, что владельцы устройств могут полностью контролировать свою безопасность.

Команда Angoka демонстрирует свое решение

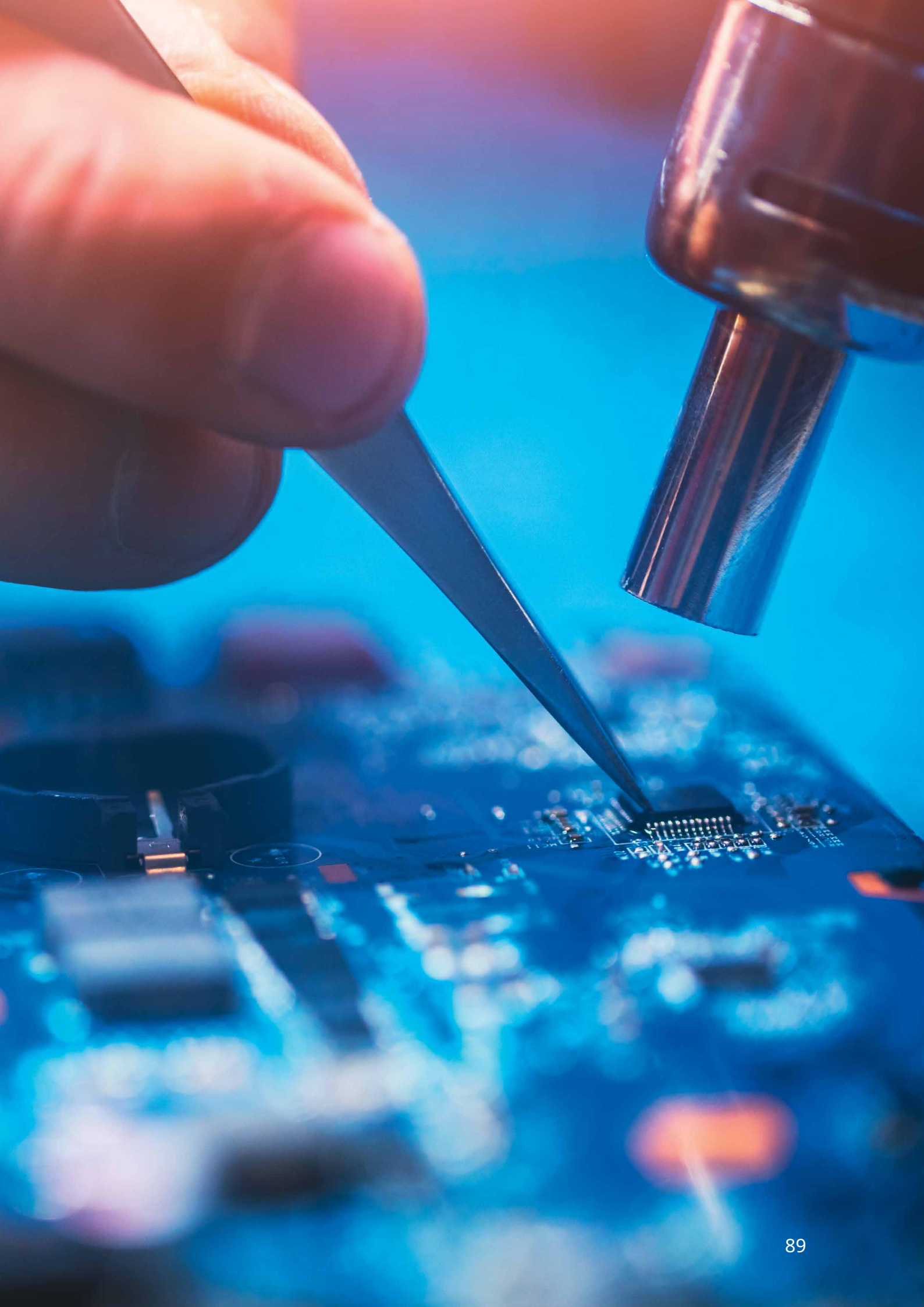
Задача 4. Объединять усилия с многосторонними организациями для разработки глобальных технических стандартов цифровых технологий в приоритетных областях, имеющих первостепенное значение для утверждения демократических ценностей, обеспечения кибербезопасности и укрепления британского стратегического преимущества с помощью достижений науки и техники.

148. Глобальные стандарты цифровых технологий являются ключевой составляющей функционирования интернета, телекоммуникационных сетей и нарождающихся технологий. То, как осуществляется разработка и развертывание этих стандартов, может влиять на наши цели в области кибербезопасности, экономическое благополучие, а также нормы и ценности. Исторически эти стандарты формировались наиболее влиятельными игроками на рынке. Кроме того, существуют материальные препятствия для участия в этой работе некоторых важных заинтересованных лиц, включая предприятия МСБ, ученых и других экспертов. К 2025 году мы достигнем следующих результатов:

149. Более активное участие широкого круга заинтересованных сторон в экосистеме глобальных технических стандартов цифровых технологий. Мы будем расширять участие заинтересованных сторон в работе основных организаций по разработке стандартов, демонстрируя ведущую роль в этом процессе на примере наших делегаций в Международном союзе электросвязи. Мы будем содействовать открытому обсуждению ключевых тенденций и факторов, которые должны принимать во внимание нормотворческие органы, на платформе Форума ООН по управлению интернетом и на других площадках. Мы усилим координацию и улучшим обмен информацией с международными партнерами, в том числе благодаря усилиям Группы контактных пунктов связи по вопросам цифровых стандартов, образованной в рамках председательства Соединенного Королевства в Большой Семерке.

150. Всемирные технические стандарты, касающиеся цифровых технологий в приоритетных для Соединенного Королевства областях, более эффективно формируются на основе демократических ценностей, факторов кибербезопасности, результатов британских исследований и инноваций в области нарождающихся технологий. Мы будем работать вместе с предприятиями отрасли, научными кругами, техническими экспертами и гражданским обществом в таких сферах, как протоколы IP, будущие сети и искусственный интеллект (ИИ), чтобы повысить осведомленность о важных факторах государственной политики в области разработки технических стандартов. Мы создадим экспериментальный центр по разработке стандартов ИИ, который будет способствовать участию Соединенного Королевств в работе по стандартизации ИИ на глобальном уровне, как предусмотрено соответствующей национальной стратегией.

151. Вся эта деятельность будет опираться на стратегические координационные механизмы в Соединенном Королевстве, такие как инициатива по сотрудничеству между правительством, Британским институтом стандартов (BSI) и Национальной физической лабораторией, описанная в Национальной стратегии развития искусственного интеллекта. Это взаимодействие будет также содействовать процветанию Соединенного Королевства за счет продвижения стандартов, благоприятствующих инновациям, росту и выравниванию возможностей.



Основополагающая цель 4: глобальное лидерство

Укрепление глобального лидерства и влияния Соединенного Королевства в интересах безопасного и благополучного мирового порядка

152. Свободное, открытое, мирное и безопасное киберпространство сохраняет свое критическое значение для укрепления коллективной безопасности и процветания, и международное взаимодействие будет и далее играть жизненно важную роль в достижении всех целей Соединенного Королевства в области кибербезопасности. Однако, чтобы отвечать требованиям эпохи системного соперничества, Соединенному Королевству потребуется играть более активную международную роль в продвижении наших интересов и ценностей в киберпространстве. Деятельность Соединенного Королевства в киберпространстве и знания кибертехнологий будут занимать центральное положение в более широкой внешнеполитической повестке правительства: мы будем проактивно использовать их для содействия построению открытого, безопасного и благополучного международного порядка.

153. Как страна, ориентированная на решение проблем и разделение бремени, мы укрепим наши основные союзы, вместе с тем сотрудничая с более широким кругом партнеров, в том числе отраслевыми предприятиями, органами глобальной технической стандартизации, гражданским обществом и научными организациями. Мы будем инвестировать средства в углубление отношений с партнерами в Африке и Индо-Тихоокеанском регионе и использовать возможности для создания новых, более гибких союзов. Как сила добра в мире, мы также продолжим расширять наш дипломатический арсенал, сочетая влияние за рубежом с достижениями в стране, используя знания в области оперативной и стратегической связи, создавая программы подготовки квалифицированных кадров и экономические партнерства. Наш подход отвечает интересам безопасности и процветания людей во всем мире, а не только в нашей стране.

Задача 1. Укреплять кибербезопасность и устойчивость международных партнеров и расширять коллективную деятельность, направленную на дестабилизацию и сдерживание противников.

154. Коллективные действия и взаимное укрепление устойчивости имеют критическое значение для успешного отражения угроз у их истоков и вместе с тем снижают мотивацию субъектов киберугроз к совершению атак на Соединенное Королевство и его партнеров. К 2025 году мы достигнем следующих результатов:

155. Международные партнеры Соединенного Королевства имеют более мощные возможности, политическую решимость, эффективное управление и системы, необходимые для расследования и устранения киберугроз и повышения устойчивости. Это приводит к снижению угрозы для британских граждан, исходящей из-за рубежа. Одной из наших приоритетных задач будет содействие наращиванию киберпотенциала в Восточной Европе, Африке и Индо-Тихоокеанском регионе, и мы продолжим сотрудничество с ключевыми союзниками на Ближнем Востоке и в Южной и Северной Америке. Мы разработаем более комплексный, основанный на усилиях всего правительства технический подход, увеличив инвестиции в наращивание экспертного потенциала в правоохранительных органах и оборонных силах и в большей мере используя возможности отраслевых и научных организаций. Мы сосредоточим усилия на защите критически важных международных цепочек поставок и объектов инфраструктуры, поощряя безопасное использование цифровых технологий и расширяя его масштабы совместными усилиями с отраслевыми партнерами.

156. Мы также активизируем усилия, направленные на развитие потенциала организаций гражданского общества, поддерживая ценностно-ориентированные дискуссии о технологиях и обществе и создавая механизмы подотчетности на местном уровне. Мы продолжим сотрудничать с эффективными многосторонними организациями и партнерами, включая Организацию Объединенных Наций, альянс «Пять глаз», НАТО, Большую Семерку, Европейский Союз, Британское Содружество Наций, ОЭСР, Глобальный форум по киберэкспертизе (GFCE), Форум АСЕАН, Африканский Союз и Всемирный Банк.

157. Чтобы эффективнее защищать интересы Соединенного Королевства и его граждан за рубежом, мы также разработаем и подготовим международную кампанию по кибергигиене для британских зарубежных представительств, которая будет адаптирована и реализована с учетом местных условий. Цель ее —ужесточить наказание за проведение вредоносной деятельности, такой как взлом, кража данных и интеллектуальной собственности и атаки программ-вымогателей. В реализации программы примут участие наши дипломаты, местный персонал, британские бизнес-сообщества на местах и непосредственные исполнители британских программ развития.

158. Более широкий международный союз, готовый и способный создавать более серьезные последствия для противников Соединенного Королевства. Мы будем содействовать повышению решимости и увеличению потенциала международного сообщества путем активизации взаимодействия на дипломатическом уровне, оперативного сотрудничества, информационного обмена и проведения совместных учений. Осуществляя взаимодействие по политическим, оперативным и правоохранительным каналам, мы усилим воздействие таких мер, как целевые киберсанкции, а также найдем новые пути для ужесточения наказания, налагаемого на субъектов киберугроз. Мы достигнем большего взаимопонимания между киберсилами ключевых союзных и партнерских стран и более эффективной интеграции кибероперациий в союзнические операции во всех доменах — на суше, в море, в воздухе, в космосе и в киберпространстве.

159. Мы продолжим содействовать наращиванию потенциала наших союзников по НАТО в области кибербезопасности в целях повышения результативности коллективных действий, в том числе путем содействия интеграции суверенных кибер-возможностей, добровольно предоставляемых Соединенным Королевством и некоторыми другими союзниками, в операции и миссии НАТО.

Задача 2. Формирование глобальной системы управления в интересах продвижения свободного, открытого, мирного и безопасного киберпространства.

160. Государства, не разделяющие ценности Соединенного Королевства, используют проблемы, связанные со свободным и открытым интернетом, для обоснования своего авторитарного видения киберпространства, прикрываясь соображениями безопасности. Соединенное Королевство примет более проактивный подход и совместно с союзниками и партнерами обеспечит разработку международных правил и механизмов в соответствии с нашими демократическими ценностями. Мы направим усилия на поддержку национального и глобального экономического роста, укрепление коллективной безопасности, поощрение ответственного использования наступательных киберсредств и создание реальных последствий для субъектов вредоносной и безответственной деятельности. К 2025 году мы достигнем следующих результатов:

161. Глобальное управление киберпространством и интернетом обеспечивает защиту британских интересов и ценностей, а Соединенное Королевство и его партнеры оказывают большее влияние на разработку и внедрение международных механизмов управления и стандартов. Мы примем более прогрессивный и проактивный подход к формированию механизмов, регулирующих киберпространство, в целях содействия глобальному экономическому росту и безопасности. Мы разработаем и предпримем практические меры, чтобы разблокировать международную дискуссию о применении правил, норм и принципов в киберпространстве и приблизиться к достижению консенсуса по эффективным мерам сдерживания деструктивной и дестабилизирующей деятельности. Мы будем добиваться этого с помощью ключевых региональных и специализированных организаций, в том числе ОБСЕ, АСЕАН и GFCE, и конструктивного взаимодействия в рамках процесса ООН, направленного на разработку нового международного договора о борьбе с киберпреступностью, который, наряду с Будапештской конвенцией обеспечивает укрепление международного сотрудничества и сохранение механизмов защиты прав человека.

162. Мы также продолжим поощрять применение Будапештской конвенции о киберпреступности, совместно с международными партнерами убедительно обосновывая сохранение ее статуса как главного международного договора в области сотрудничества. Мы продолжим продвигать и расширять деятельность многосторонних организаций по регулированию интернета, таких как Корпорация по управлению доменными именами и IP-адресами (ICANN), и Форум ООН по управлению интернетом (IGF). Эти усилия будут дополнены нашей деятельностью по формированию глобальных стандартов цифровых технологий (описанных в главе о технологиях) и по увеличению экспорта британских технологий кибербезопасности (как описано ниже), что также будет содействовать внедрению британских стандартов в кибернетические экосистемы других стран.

163. Большинство стран, придерживающихся умеренной позиции, поддерживают и продвигают британское видение киберпространства и будущего интернета, и более эффективно противостоят влиянию авторитарных государств на многостороннюю систему. Мы продемонстрируем, что можно противостоять вызовам в киберпространстве, не прибегая к авторитарным подходам, и вместе с тем содействовать инновациям, развитию и росту. Мы поможем странам, испытывающим трудности с цифровизацией, наработать широкий спектр знаний в области права и стратегических коммуникаций, необходимых для участия в международной дискуссии и внедрения согласованных механизмов. Мы будем вскрывать случаи безответственного использования кибер-возможностей и укреплять доверие на международном уровне. Мы продолжим демонстрировать применение открытого и транспарентного подхода к использованию наступательных кибер-возможностей везде, где это возможно, укрепляя репутацию Соединенного Королевства как силы добра.

Задача 3. Использовать и экспортировать британские средства и знания в области кибербезопасности в целях укрепления нашего стратегического преимущества и продвижения интересов в области внешней политики и процветания в целом.

164. В ответ на системное соперничество и стремительный технологический прогресс британская деятельность и возможности в киберсекторе будут рассматриваться, наряду с другими источниками национальной мощи, как средства укрепления стратегического преимущества и достижения целей в области внешней политики и процветания. Наша цель — построение международного порядка, в котором созданы условия для процветания отрытого общества и экономики и защищены права человека на фоне повышения благосостояния страны. К 2025 году мы достигнем следующих результатов:

165. Наша деятельность в киберпространстве и в отношении киберпространства способствует повышению глобальной стабильности и защите основанной на правилах международной системы, открытого общества и демократических систем там, где подрывают их основы. Мы проведем основанную на ценностях международную кампанию по защите прав человека и укреплению культурного разнообразия и гендерного равенства в области разработки, развития и использования киберпространства. Сюда входит, помимо прочего, противодействие отключениям интернета, борьба с предвзятостью в алгоритмах искусственного интеллекта и повышение безопасности в интернете. Мы будем более эффективно конкурировать, чтобы защищать демократические ценности, системы и процессы, а также укреплять основанную на правилах международную систему (включая Организацию Объединенных Наций, Всемирную организацию здравоохранения и глобальную систему торговли), продолжая инвестировать в нашу сеть киберспециалистов, охватывающую шесть континентов. Мы будем более широко использовать стратегические коммуникации для поддержки британских программ научного сотрудничества и обмена и содействовать переводу британских идей в практическое русло.

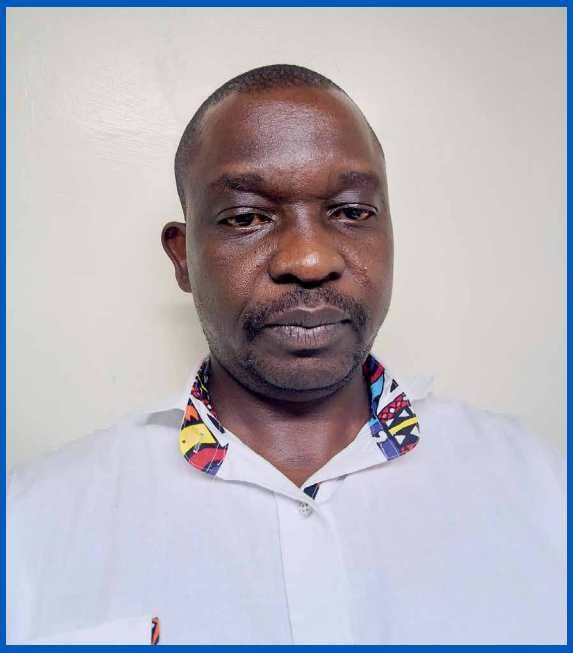
166. Соединенное Королевство — один из 3-х ведущих мировых экспортеров киберрешений и киберэкспертизы: наша кибериндустрия считается одним из самых востребованных поставщиков решений кибербезопасности для иностранных правительств и крупных коммерческих клиентов. Мы будем демонстрировать лучшие британские решения в области кибербезопасности путем активизации межправительственного взаимодействия под эгидой Программы специальных представителей по кибербезопасности и международной сети контактов. Мы будем оказывать поддержку компаниям по всему Соединенному Королевству на всех этапах, от разработки инноваций до экспорта, помогая им стать компетентными экспортерами и привлекать внешние инвестиции, а также будем более активно поддерживать предприятия МСБ, в том числе в рамках нового Факультета экспорта.[32] [33] Наряду с деятельностью в рамках Cyber Growth Partnership и других программ и инициатив, описанных в главе о британской кибернетической экосистеме, мы также создадим новое Управление кампаниями по развитию киберпотенциала, призванное обеспечить более организованную и скоординированную поддержку основных кампаний по содействию экспорту.

---

[32] См. описание в Британской стратегии инноваций (2021)

[33] Факультет экспорта при Управлении по содействию британскому экспорту в сфере обороны и безопасности (UKDSE) — онлайн-платформа для обучения и развития, предназначенная для предприятий МСБ в секторе обороны и безопасности, имеющая специализированные модули для компаний по кибербезопасности. Регистрация на Факультете обеспечивает доступ к учебным модулям, разработанным на основе учебных планов, а также к ценной информации о мероприятиях и деятельности Управления по содействию британскому экспорту в сфере обороны и безопасности.

Чарльз Джума, Британская программа по содействию доступу к цифровым технологиям в Найроби



Меня зовут Чарльз Весонга Джума. Я возглавляю работу по подготовке и реализации программ в области кибербезопасности, цифрового развития, инклюзивности и предпринимательства в рамках глобальной и межправительственной Программы Соединенного Королевства по содействию доступу к цифровым технологиям в Кении. Я также оказываю поддержку дополнительным проектам, финансируемым из средств Кибер-портфеля Фонда предотвращения конфликтов, содействия стабильности и безопасности (CSSF). Значение безопасного интернета, безопасности, защиты данных и ответственного использования киберпространства переоценить невозможно. Пандемия COVID-19 показала, что интернет-безопасность и кибергигиена имеют такое же значение, как здравоохранение и общественная гигиена. Я горячо поддерживаю необходимость защиты каждого человека от интернет-угроз и ущерба в рамках общей деятельности британского правительства по наращиванию кибермощи.

Сара Мерчант, сотрудник по вопросам кибербезопасности при посольстве Соединенного Королевства в Тбилиси

Меня зовут Сара, и я работаю в посольстве Соединенного Королевства в Тбилиси на должности сотрудника по вопросам кибербезопасности, осуществляя тесное взаимодействие с правительством Грузии и британским центром NCSC. В ходе повседневной работы мне приходится заниматься разными вопросами — от контактов на политическом уровне и содействия внедрению новой киберстратегии до привлечения британских специалистов к деятельности по укреплению технического потенциала Грузии. Для меня большая честь быть на переднем крае процесса проецирования британских экспертных знаний и оказания поддержки Грузии в повышении устойчивости перед лицом киберугроз. Мы можем многому научиться у Грузии, которая, к сожалению, испытала на себе серьезные последствия враждебной деятельности. Наша работа помогает обеим странам стать сильнее и повысить свою устойчивость и информированность.

Основополагающая цель 5: противодействие угрозам

Обнаружение, дезорганизация и сдерживание наших противников в целях укрепления безопасности Соединенного Королевства в киберпространстве и с его помощью

167. Стоящие перед нами угрозы имеют сложную природу. Обеспокоенность вызывают угрозы в киберпространстве (например, при пользовании интернетом), угрозы Соединенному Королевству и его партнерам с помощью киберпространства (например, угрозы для британской сети объектов критической национальной инфраструктуры) и угрозы для функционирования фундаментальной международной киберинфраструктуры. Все эти угрозы могут повлиять на доступность услуг, важных для людей, или на конфиденциальность или целостность данных и информации, которые передаются по этим системам. Основы этого подхода к противодействию угрозам коренятся в необходимости повышения киберустойчивости, как говорилось ранее в этом документе. В этой главе описывается, как мы будем добиваться ужесточения наказания и повышения рисков, связанных с атаками на Соединенное Королевство в киберпространстве, а также реализации нашего полного потенциала как кибердержавы.

168. Со времени принятия Национальной стратегии кибербезопасности 2016–2021 года мы кардинально изменили подход к снижению угроз. Мы создали первоклассные возможности для обнаружения и анализа угроз в рамках Национального центра кибербезопасности (NCSC). Вместе со своими партнерами в государственном и частном секторе, как внутри страны, так и за рубежом, NCSC работает над обнаружением угроз и инцидентов и реагированием на них. Как участник разведывательного сообщества, NCSC предоставляет политикам информацию, необходимую для присвоения ответственности за атаки против британских интересов, которое является критически важной составляющей нашего подхода к сдерживанию киберугроз. Мы вложили значительные средства в наступательный киберпотенциал в ходе реализации Национальной программы наступательных кибероперацій, а недавно — в создание Национальных силы кибербезопасности (NCF). Мы также разработали комплексные национальные меры реагирования

правоохранительных органов, принимаемые под руководством Национального агентства по борьбе с преступностью (NCA), и прилагаем усилия, чтобы обеспечивать ужесточение наказания, связанных с осуществлением враждебной и преступной деятельности в киберпространстве. Мы создали первоклассные возможности для обнаружения и оценки угроз и средства, позволяющие транслировать полученную аналитическую информацию в эффективные меры смягчения рисков в масштабе государственного и частного секторов. Мы разработали автономный режим киберсанкций в качестве еще одного средства наложения наказания на наших противников. Благодаря сочетанию дипломатического взаимодействия и усилий NCSC, служб безопасности и разведки, NCA, правоохранительных органов в целом и NCF мы добились уменьшения воздействий, вызванных угрозами, в реальном мире путем принятия мер, направленных на прямое противодействие противникам, предотвращение атак и снижение наносимого ущерба.

169. Однако угрозы становятся все более изощренными, сложными и серьезными; и наши усилия еще не привели к фундаментальным изменениям в калькуляции рисков для нападающих, которые продолжают осуществлять успешные атаки на Соединенное Королевство и его интересы. Мотивами для кибератак на Соединенное Королевство являются шпионаж, получение преступных доходов и коммерческих, финансовых и политических выгод, саботаж и дезинформация. Преступники разрабатывают возможности, позволяющие им обходить внедряемые меры снижения рисков; все более сложные киберинструменты и вспомогательные средства становятся доступным товаром в этом растущем секторе, способствуя снижению барьеров для осуществления вредоносной деятельности злоумышленниками любого рода. С повышением способности злоумышленников похищать и шифровать ценные данные и вымогать выкуп, подрывая деятельность компаний и ключевых государственных служб, киберпреступность становится более прибыльной. Это приводит к тому, что злоумышленники все чаще получают финансовые выгоды, используют конфиденциальность и свободу слова в своих интересах и пытаются манипулировать событиями с помощью дезинформации.

170. Таким образом, британский подход сместится в сторону проведения кампаний на более комплексной и долгосрочной основе, связанных с рутинным, комплексным и креативным использованием всего спектра доступных рычагов и возможностей, которые позволяют налагать наказание на наших противников, преследовать их, пресекать преступные действия и сдерживать будущие атаки. Три ключевых элемента, на которые опирается этот подход:

- постоянное развитие NCF как следующего этапа в укреплении способности Соединенного Королевства осуществлять наступательные кибероперации против его противников;

- специализированные межведомственные кампании по преодолению угроз для Соединенного Королевства с использованием дипломатических, военных, разведывательных, правоохранительных, экономических, юридических и стратегических коммуникационных инструментов;

- новые инвестиции в укрепление способности правоохранительных органов проводить масштабные и оперативные расследования и сохранять техническое преимущество перед нашими противниками, позволяющее предотвращать преступления и обнаруживать серьезных преступников и вспомогательные сервисы, которыми они пользуются;

- активизация деятельности в области обмена данными в масштабах правительства и отрасли, как описано в главе об устойчивости.

171. Киберпространство создает возможности для Соединенного Королевства, открывая новые пути для активного продвижения наших национальных интересов. Например, наступательные кибероперации предусматривают целый ряд гибких и масштабируемых деэскалационных мер, которые будут способствовать сохранению Соединенным Королевством стратегического преимущества и решению приоритетных национальных задач таким образом, чтобы избежать необходимости подвергать людей риску физического вреда.

172. Мы продолжим разрабатывать наступательные кибер-возможности и вкладывать средства в них в рамках деятельности NCF. NCF значительно укрепит способность Соединенного Королевства к успешному противостоянию противникам в киберпространстве и в реальном мире, чтобы защитить страну, ее народ и наш образ жизни. Мы, как сила добра, будем ответственно использовать эти возможности наряду с дипломатическими, экономическими, судебными и военными рычагами власти. Мы будем использовать их в интересах поддержки и продвижения широкого спектра государственных приоритетов в области национальной безопасности и экономического благополучия, а также содействия предотвращению и обнаружению серьезных преступлений.

Задача 1. Предпринимать меры для выявления государственных, криминальных и других субъектов киберпреступлений, расследования их вредоносной деятельности и обмена информацией в целях защиты Соединенного Королевства, его интересов и граждан.

173. К 2025 году мы достигнем следующих результатов:

174. У правительства есть глубокое понимание кибер-возможностей, которыми располагают государственные, преступные и другие субъекты вредоносной кибердеятельности, и их стратегического замысла в отношении Соединенного Королевства. Чтобы углубить понимание киберугроз, мы сохраним и будем повышать уровень крупных инвестиций в разведывательные службы и правоохранительные органы, предусмотренных стратегией 2016 года. В частности, мы повысим способность правоохранительных органов понимать и устранять угрозы киберпреступности, в том числе ее связи с государственными и иными международными и внутренними угрозами и технологическими вспомогательными средствами, что поможет нам разрабатывать более эффективные политические меры реагирования. Мы улучшим координацию действий по обнаружению угроз в масштабах всего правительства при помощи общей стратегии доступа к данным и использования их всеми разведывательными службами и правоохранительными органами. Мы сосредоточим внимание на понимании замысла противников и критериев принятия ими решений, а также воздействий, которые наша деятельность оказывает на них, в том числе, того, как люди становятся киберпреступниками и что мы можем предпринять, чтобы предотвратить это.

175. Достижению этих результатов будет способствовать наша деятельность по созданию возможностей для более оперативного и простого уведомления о киберинцидентах, как описано в главе об устойчивости.

176. Осуществляется рутинное и всеобъемлющее расследование наиболее серьезных угроз, исходящих от государственных, криминальных и других субъектов, с использованием всех источников информации и общего опыта и знаний правительства, правоохранительных органов и частного сектора. Мы будем наращивать разведывательный, операционный и технический потенциал сети подразделений кибербезопасности в британских правоохранительных органах. Мы будем вкладывать средства в кибер-разведывательные возможности NCA, используемые для борьбы с организованными преступными группировками, в инициативу по наращиванию регионального разведывательного потенциала, которая улучшит доступ к разведывательным данным в масштабах Соединенного Королевства и передачу их, и в развитие навыков и способностей, необходимых правоохранительным органам для расследования и пресечения кибер- и цифровых преступлений.

177. Расследования будут опираться на разведывательные данные из всех источников и на использование навыков и знаний частного сектора, в том числе

путем содействия компаниям в передаче данных правоохранительным органам. Мы продолжим выполнять рекомендации HMICFRS в отношении правоохранительных мер реагирования на киберпреступления, чтобы сохранить прочную основу для сети борьбы с киберпреступностью на национальном, региональном и местном уровне.[34]

178. Регулярно осуществляется масштабный и оперативный обмен информацией и данными об угрозах, и повышается способность тех, кто получает их, принимать меры. NCSC опробовал ряд инициатив по созданию более эффективных сообществ по защите сетей в широком ряде секторов, которые не только получают информацию об угрозах и могут обмениваться ею, но и способны все эффективнее использовать ее на общее благо. Мы расширим эту деятельность, изначально сосредоточив усилия на том, чтобы помочь государству повысить эффективность своей защиты, при поддержке Правительственного координационного центра кибербезопасности (описанного в главе об устойчивости). Координационный центр кибербезопасности финансового сектора уже прокладывает путь вперед в частном секторе.[35]

179. NCSC также изучает пути для отслеживания нарождающихся угроз и продолжит работать с Институтом Алана Тьюринга над изучением возможностей для обнаружения некоторых видов кибератак с помощью машинного обучения. Результаты этих исследований будут и далее помогать нам лучше понять, как мы можем использовать искусственный интеллект для обнаружения фактов вредоносной деятельности.

[34] Инспекторат корпуса констеблей, пожарной и спасательной служб Её Величества
[35] NCSC, Financial sector cyber collaboration centre (FSCCC) (2021)

Пресечение киберпре-ступности также ведет к пресечению других видов преступной деятельности

Киберпреступления (согласно определению Закона о неправомерном использовании компьютерных технологий) имеют место, когда осуществляются: несанкционированный доступ к компьютерам, сетям и другим цифровым устройствам, сопутствующие деяния, причиняющие ущерб, или изготовление либо поставка инструментов для совершения этих преступлений. Это дает преступникам возможность совершать другие вредоносные действия в киберпространстве, такие как атаки с использованием программ-вымогателей, получение несанкционированного доступа к учетным записям, кража интеллектуальной собственности, атаки типа «отказ в обслуживании» или хищение больших наборов персональных данных — это серьезные преступления, число которых постоянно растет.

Киберпреступность против граждан часто проявляется в форме других преступлений, совершению которых она содействует и способствует. Несанкционированный доступ к компьютерам может привести к совершению различных преступлений — мошенничества, кражи, сексуального шантажа и в некоторых случаях содействовать сталкингу, домашнему насилию и притеснениям. Все эти преступления наносят серьезный вред британским гражданам на ежедневной основе, разрушая компании и разбивая жизни. Поэтому киберпреступность стоит отдельно и отличается от проблем, связанных с интернет-безопасностью в целом, таких как запугивание и притеснение, использование риторики ненависти, распространение дезинформации, пропаганда бандитской культуры и насилия и предоставление несовершеннолетним лицам доступа к порнографии. Правительство предусматривает решение этих проблем в официальных документах о причинении вреда онлайн и в проекте закона об интернет-безопасности.

Задача 2. Предпринимать меры для сдерживания государственных, криминальных и других субъектов киберпреступлений и противодействия их вредоносной деятельности, направленной против Соединенного Королевства, его интересов и граждан.

180. К 2025 году мы достигнем следующих результатов:

181. Осуществление кибератак на Соединенное Королевство стало более затратной и опасной деятельностью для государственных, криминальных и других вредоносных кибер-субъектов. Мы будем проводить долгосрочные специализированные кампании с использованием всего спектра возможностей Соединенного Королевства (включая дипломатические, экономические, скрытые и открытые рычаги) для воздействия на поведение вредоносных и других преступных кибер-субъектов. В частности, мы будем более эффективно демонстрировать противникам наши возможности и готовность налагать существенное наказание, в том числе путем применения санкций и проведения операций силами правоохранительных органов и NCF. В рамках программы NCA Cyber Choices мы будем принимать меры, чтобы не допускать вовлечения граждан в киберпреступную деятельность, разрабатывая, совместно с представителями отрасли и научных кругов, более привлекательные варианты для потенциальных правонарушителей, такие как ученичество и стажировка.

182. Мы также предоставим правоохранительным органам и разведывательным службам необходимые средства и полномочия в рамках Законопроекта о противодействии государственным угрозам, а также путем обновления существующего законодательства и закрепления новых видов преступлений с учетом эволюции государственных угроз. Кроме того, мы внесем поправки в Закон 2002 года о преступных доходах, которые позволят оптимизировать способность правоохранительных органов к розыску, аресту и возвращению доходов от киберпреступности. В этой связи мы предусмотрим, в частности, создание полномочий на конфискацию имущества в гражданско-правовом порядке, что позволит снизить риски, создаваемые лицами, которых невозможно привлечь к ответственности.

183. Государственным, криминальным и другим вредоносным субъектам киберпреступлений стало сложнее осуществлять атаки на Соединенное Королевство в результате нашей успешной деятельности, направленной на подрыв их возможностей и порицание их действий. Мы пересмотрим политику правительства и оперативный подход к борьбе с программами-вымогателями, сосредоточиваясь на этой проблеме при проведении приоритетных кампаний в сотрудничестве с представителями отрасли и международными партнерами. Мы активизируем партнерство между NCF, NCSC, NCA, правоохранительными органами, дипломатическими службами и разведывательным сообществом, направленное на противодействие угрозам для конфиденциальности, целостности и доступности киберпространства или данных и услуг в киберпространстве. В частности, мы будем вкладывать средства в возможности для поражения инфраструктуры, используемой киберпреступниками, и задействуем наш правоохранительный и наступательный киберпотенциал для пресечения вредоносной кибердеятельности. Наши противники наращивают кибер-возможности и все чаще используют их в злонамеренных целях. Мы будем использовать весь потенциал NCF там, где это целесообразно, для подрыва этих усилий, а также для обороны и защиты Соединенного Королевства.

184. Мы также будем препятствовать передаче высокотехнологичных возможностей государствам и организованным криминальным группировкам по коммерческим и криминальным рыночным каналам, принимая меры в отношении форумов, которые благоприятствуют и способствуют совершению киберпреступлений и представляют киберпреступность в привлекательном виде.

185. Повысилась эффективность уголовного правосудия и результативность других мер противодействия киберпреступности за счет более эффективного использования потенциала уголовного правосудия для судебного преследования киберпреступников в Соединенном Королевстве. Мы пересмотрим Закон о неправомерном использовании компьютерных технологий (CMA) и соответствующие полномочия, необходимые правоохранительным органам для успешного расследования новых и нарождающихся угроз, исходящих со стороны преступников, и подготовим больше прокуроров, специализирующихся на киберпреступлениях, число которых постоянно растет. Мы также будем содействовать усовершенствованию специализированных навыков персонала правоохранительных органов, отрабатывая и внедряя их в широкую практику, чтобы обеспечить постоянный приток специалистов, обладающих необходимыми специализированными знаниями в области кибербезопасности, в рамках учебных программ Национального совета начальников полиции (NPCC) по развитию кибернавыков и программы Полицейского колледжа по подготовке специалистов по цифровой и кибербезопасности (Cyber Digital Career Pathways).

Сьюзен Муди, сотрудник подразделения по предотвращению преступности, Служба полиции Северной Ирландии (PSNI)

(Слева направо) Сьюзен Муди (PSNI), Сара Траверс (телеведущая) и Джо Доулан (глава Центра кибербезопасности Северной Ирландии)

Компьютеры и мобильные устройства — неотъемлемый атрибут повседневной жизни молодежи. Они открывают широкие возможности, но вместе с тем представляют опасность при злоупотреблении этими возможностями. Подразделение PSNI по предотвращению преступности принимает необходимые меры вмешательства на ранних этапах, помогая молодым людям понять законы, касающиеся использования и неправомерного использования компьютеров. Это позволяет привлечь внимание к опасным признакам потенциального вовлечения в преступную деятельность и к возможностям, которые открывают такие инициативы как CyberFirst и программы по выбору карьеры в киберсекторе. Они позволяют заинтересованным или талантливым молодым людям выбрать альтернативу преступности, а также предотвращать злоупотребления со стороны других лиц, осуществляемые в преступных целях. Сьюзан неустанно работает над разработкой школьной информационной программы по кибербезопасности для использования во всех средних школах и имеет прямые связи более чем с 40 начальными школами, многочисленными средними школами, молодежными организациями и другими организованными группами. Эти молодые люди вполне могут стать поборниками кибербезопасности и защитниками будущего.

Задача 3. Предпринимать действия в киберпространстве и с его помощью в интересах национальной безопасности, а также предупреждения и выявления серьезных преступлений.

186. К 2025 году мы достигнем следующих результатов:

187. Кибер-возможности Соединенного Королевства более эффективно используются для сдерживания и ликвидации угроз, не связанных с киберпреступностью. Мы будем наращивать и развивать Национальные силы кибербезопасности, обеспечив реализацию долгосрочного видения этого ключевого элемента нашего потенциала, обеспечивая его полную интеграцию с Центром правительственной связи (GCHQ), Министерством обороны (МО), Секретной разведывательной службой (SIS) и Лабораторией оборонной науки и техники и тесно сотрудничая с правоохранительными органами и правительственными службами в целом. Мы будем проводить законные и пропорциональные наступательные кибероперации с использованием Национальных сил кибербезопасности, а также ответственно действовать в киберпространстве, подавая пример другим. Мы будем и далее проводить наступательные кибероперации в поддержку национальной безопасности Соединенного Королевства, в том числе нашей оборонной и внешней политики, а также в целях предотвращения серьезных преступлений.

188. Мы также будем наращивать и развивать технические возможности правоохранительных органов для принятия мер противодействия в области инфраструктуры и криптовалюты, которые можно применять против других угроз.

189. Кибер-возможности Соединенного Королевства встроены в полный спектр оборонных операций в соответствии с Концепцией интегрированных операций 2025 года.[36] Мы сохраним конкурентное преимущество перед противниками в военной области и будем содействовать расширению сотрудничества с союзниками и партнерами. Мы продолжим реализацию Программы изменений, ориентированной на многодоменную интеграцию в оборонной области, которая обеспечит объединение возможностей в масштабе всех доменов и повышение уровня интеграции с другими орудиями, составляющими нашу национальною мощь, а также усилит наше военное преимущество перед противником. Кибербезопасность станет одной из основных составляющих оборонного бизнеса благодаря подготовке высококвалифицированных киберспециалистов, общей осведомленности персонала оборонного сектора о кибербезопасности, а также передовым и устойчивым кибер-возможностям.

[36] Министерство обороны, Integrated Operating Concept (2020)

Расследование правоохранительными органами серьезных киберпреступлений

Операция Imperil: Операция Imperil — совместное расследование Юго-Восточного регионального подразделения по борьбе с организованной преступностью (SEROCU) и ФБР в отношении вебсайта, на котором продавались скомпрометированные персональные и банковские данные людей, ставших жертвами кибератак. Злоумышленники покупали персональные данные и использовали их для совершения мошеннических действия и других правонарушений, связанных с неправомерным использованием компьютерных технологий. В результате масштабного расследования были выявлены банковские счета и платежи за техническую инфраструктуру, на основании которых было установлено, что владелец вебсайта находится в Пакистане. Это позволило ФБР провести тайную операцию и наложить арест на этот вебсайт, а затем закрыть его. Юго-Восточное региональное подразделение по борьбе с организованной преступностью арестовало главного подозреваемого из Соединенного Королевства, который, как было установлено, открыл счет в американском банке от имени владельца вебсайта для отмывания преступных денег. Подозреваемый британский гражданин совершил крупное мошенничество с использованием скомпрометированных данных — открывал банковские счета на чужие имена, использовал скомпрометированные банковские счета для оплаты роскошного отдыха и подавал фальшивые заявления в Министерство труда и пенсий, причинив государству ущерб на сумму более 90 тысяч фунтов стерлингов. Подозреваемому предъявили обвинение по девяти случаям нарушения закона и приговорили к четырем годам лишения свободы, сократив этот срок в связи с признанием вины на ранней стадии. Следственная группа была удостоена похвалы судьи. На момент публикации этого документа ходатайство о конфискации и пожизненном применении Закона о преступных доходах находилось в стадии рассмотрения.

Операция Nipigon: Это расследование Службы столичной полиции в отношении гражданина Болгарии, подозреваемого в создании уникальных фишинговых страниц. Ущерб для Соединенного Королевства оценивается в сумму более 40 млн фунтов стерлингов. Этот гражданин попал в поле зрения правоохранительных органов в ходе расследования деяний другого хорошо известного киберпреступника, приговоренного в 2018 году к 10 годам лишения свободы, который использовал фишинговые страницы, созданные вышеуказанным гражданином Болгарии, в своих преступных целях. Расследование было инициировано после обнаружения важного в этом контексте адреса электронной почты, связанного с подозреваемым. По результатам длительных и сложных следственных мероприятий было налажено взаимодействие с болгарскими органами, и подозреваемый был арестован и выдан Соединенному Королевству. После ознакомления со всеобъемлющими следственными материалами он признал свою вину по всем выдвинутым обвинениям и был приговорен к девяти с половиной годам лишения свободы.

Операция Leasing. В 2020 году на пике пандемии COVID-19 NCA возглавило расследование угрозы бомбового терроризма против NHS с вымогательством злоумышленником платежей в биткойнах (BTC). Совместно с немецкими правоохранительными органами сотрудники NCA установили личность и задержали подозреваемого, который был успешно осужден в немецком суде.

12 апреля 2020 года гражданин Италии, проживающий в Германии, отправил по сети TOR электронное сообщение с заявлением о намерении взорвать бомбу в больнице NHS, если он не получит 10 млн фунтов стерлингов в биткойнах.

NCA оперативно придало этому расследованию статус высокоприоритетного и поручило специалистам по расследованию киберпреступлений установить личность злоумышленника и предотвратить возможную атаку.

Злоумышленник также отправил электронные сообщения с угрозами нападения на членов парламента и взрыва бомбы во время протеста сторонников движения Black Lives Matter в Лондоне. Несмотря на то, что электронные сообщения были написаны по-английски, следователи NCA, опираясь на специализированные методы расследования киберпреступлений, а также на результаты поведенческого и лингвистического анализа, установили, что родным языком злоумышленника, по всей вероятности, является немецкий.

Совместно с немецкими правоохранительными органами сотрудники NCA установили, что электронные сообщения были отправлены с компьютера с берлинским ip-адресом. Благодаря международному сотрудничеству и несмотря на серьезные попытки злоумышленника скрыть свою личность и местонахождение, следователям удалось установить его личность, и сотрудники немецких правоохранительных органов установили за ним наблюдение. 15 июня 2020 года подозреваемый был задержан и заключен под стражу по обвинению в попытке вымогательства. 26 февраля 2021 года его приговорили к трем годам лишения свободы.

Борьба с терроризмом с помощью киберпространства

Кампания по противодействию Даиш. Деятельность Министерства обороны и GCHQ, направленная против Даиш, — это пример активного противодействия угрозам со стороны тех, кто неправомерно использует возможности интернета и современных средств связи.

Даиш потратил много времени и сил на разработку технологий, позволяющих создавать медиаконтент для использования в целях радикализации населения и пополнения своих рядов, а также для поощрения террористических атак во всем мире. В последние годы мы наблюдали результаты применения этого подхода по всей Европе, включая атаки в Лондоне и Манчестере. Даиш также использовал современные системы связи для целей командования и управления своими боевыми операциями. Это позволило ему обеспечивать гибкость, масштабность и оперативность операций, а также создавать еще большую опасность для населения, которое они стремились контролировать, и максимально расширять сферу влияния так называемого халифата.

В ходе битвы за Мосул — самопровозглашенной столицы Даиш — в рамках поддержки действий коалиции и более широкой кампании с применением всего спектра боевых действий мы использовали средства и методы ведения кибероперациий наряду с военными. Результаты этих операций имели широкий масштаб. Нарушение связи, развенчание пропаганды, подрыв доверия внутри групп и лишение доступа к оборудованию и сетям, используемым в ходе их операций, — все это было использовано для снижения эффективности операций Даиш. Мы также могли использовать кибер-методы, чтобы донести информацию правительства Соединенного Королевства до целевой аудитории или обратить внимание тех, кто, сами того не подозревая, могли оказывать помощь Даиш, на их действия. Эти операции внесли существенный вклад в усилия коалиции, направленные на подавление пропаганды Даиш, ограничение его способности координировать атаки и на защиту сил коалиции на поле боя.

Эндрю, член Национальных сил кибербезопасности

Меня всегда привлекали новейшие передовые технологии. До работы в разведывательных службах я служил в полиции, где прошел путь от патрульного полицейского до специалиста по цифровой криминалистической экспертизе. В мои обязанности на этой должности входил поиск доказательств в электронных устройствах подозреваемых. Мне это очень нравилось, но я хотел узнать, какие еще возможности существуют.

По окончании школы я не поступал в ВУЗ, и мой выбор карьеры до сих пор определяло естественное любопытство. Это можно сказать обо всех моих коллегах в Национальных силах кибербезопасности. У них у всех разный предыдущий опыт. В центре всего — обладающие глубокими знаниями технические эксперты, но среди нас также есть бывший менеджер супермаркета, учитель начальной школы и пожарник. При этом нас всех объединяет способность к непредубежденным суждениям, жажда знаний и общая цель — обеспечить безопасность страны, оценивая угрозы и возможности, которые нарождающиеся технологии создают для национальной безопасности.

Работая в полиции я гордился тем, что могу помогать людям на персональном уровне. Сегодня, работая в составе этой уникальной команды в Национальных силах кибербезопасности, я стал частью силы добра во всем мире.

Реализация наших амбициозных целей

190. Настоящая стратегия не будет иметь никакого значения при отсутствии эффективного подхода к реализации ее целей, мониторингу и оценке прогресса в их достижении, а также без механизмов корректировки курса в случае необходимости. В этой главе изложен наш подход к реализации.

Роли и обязанности государственных учреждений и организаций

191. Национальная киберстратегия является одной из ряда субстратегий, которые в своей совокупности будут обеспечивать достижение амбициозных целей, поставленных в Интегрированном обзоре. Совет национальной безопасности будет пользоваться полномочиями министерского надзора в отношении этих стратегий, осуществляя мониторинг их реализации и принимая во внимание общий баланс и направление стратегии Соединенного Королевства. Оценка прогресса в достижении целей этой стратегии будет осуществляться с помощью Механизма государственного планирования и оценки результатов и Планов по достижению результатов.

192. Все министры будут играть определенную роль в укреплении позиции Соединенного Королевства как ответственной и демократической кибердержавы, способной защищать и продвигать свои интересы в киберпространстве и с его помощью. Сюда входят конкретные наборы обязанностей министров на ведущих ролях либо в области осуществления или координации усилий по достижению одной или нескольких из пяти основополагающих целей Национальной киберстратегии, либо в области контроля за наращиванием наиболее важных кибер-возможностей и выполнением решений.

- **Канцлер герцогства Ланкастерского,** при поддержке **государственного казначея**, обеспечивает общее руководство в масштабе всех ведомств, гарантируя эффективное реагирование правительства на киберугрозы и достижение наших амбициозных целей как кибердержавы. Сюда входит разработка и реализация Национальной киберстратегии, программы инвестиций в ее поддержку и координация усилий правительства по укреплению киберустойчивости. Он также отвечает за общую межсекторальную политику и координацию деятельности,

направленной на повышение кибербезопасности и устойчивости критической национальной инфраструктуры Соединенного Королевства. Канцлер герцогства Ланкастерского по умолчанию выступает в роли председателя на министерских совещаниях COBR по киберинцидентам, которые проводятся в случае необходимости.

- **Британский министр внутренних дел** играет ключевую роль в реализации Национальной киберстратегии в целом, в том числе в реагировании на киберинциденты, в соответствии со своими обязанностями по обеспечению государственной безопасности. Министр внутренних дел возглавляет деятельность правительства по обнаружению, пресечению и сдерживанию противника, наряду с министром иностранных дел, по делам Содружества и развития и министром обороны и осуществляет общую координацию этой деятельности. Он, в частности, отвечает за борьбу с киберпреступностью.

- **Согласно законодательству, министр иностранных дел, по делам Содружества и развития** отвечает за вопросы, касающиеся GCHQ и, следовательно, Национального центра кибербезопасности. Министр иностранных дел возглавляет деятельность правительства по укреплению ведущей глобальной роли Соединенного Королевства в области кибертехнологий и, в частности, отвечает за присвоение ответственности за киберпреступления, применение режима санкций и привлечение международного сообщества к реагированию на киберинциденты высокой категории. Министр иностранных дел также возглавляет деятельность правительства по обнаружению, пресечению и сдерживанию противника, наряду с министром внутренних дел и министром обороны.

- **Министр обороны** возглавляет деятельность правительства по обнаружению, пресечению и сдерживанию противника наряду с министром иностранных дел, по делам Содружества и развития и министром обороны.

- **Министр иностранных дел, по делам Содружества и развития и министр обороны** отвечают за Национальные силы кибербезопасности, созданные совместными усилиями оборонных ведомств и разведывательных служб.

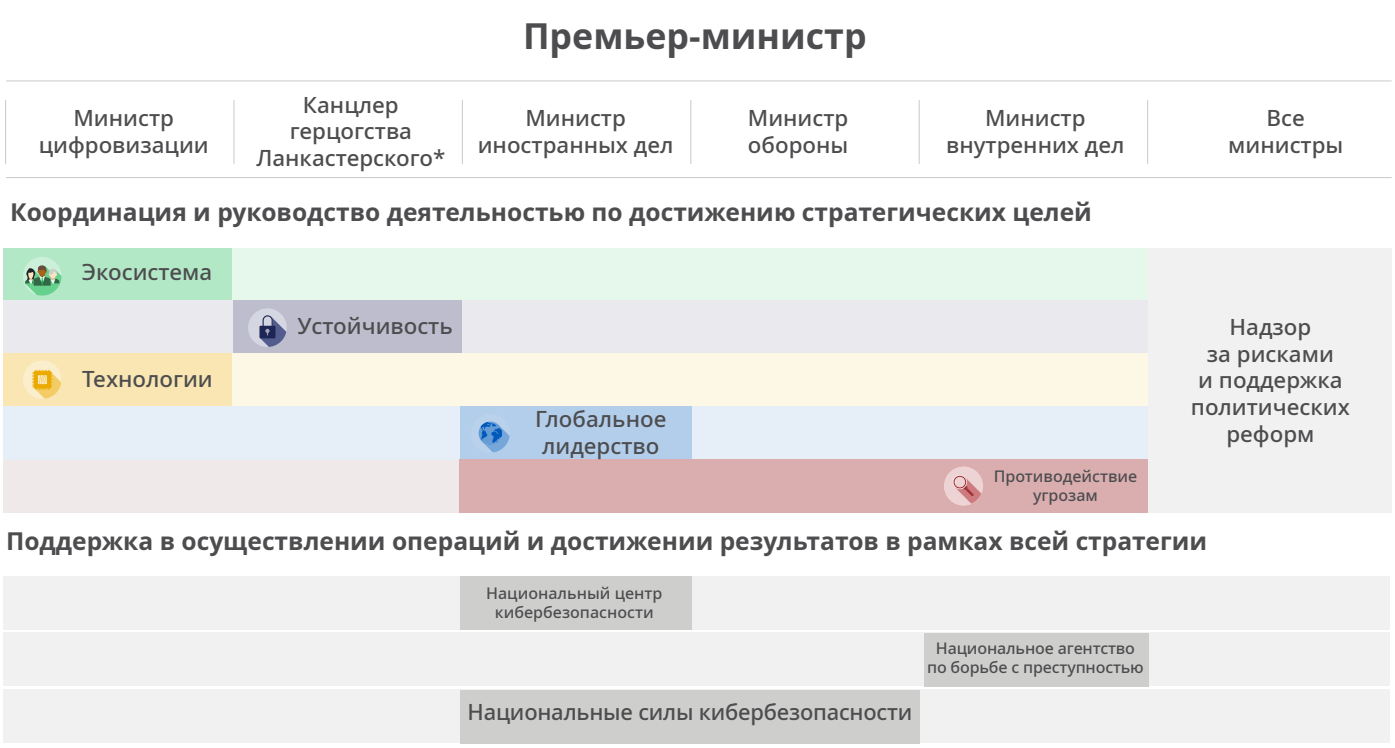
- **Министр цифровизации, культуры, СМИ и спорта** возглавляет деятельность по обеспечению кибербезопасности организаций в различных секторах экономики в той мере, в которой это касается цифровой политики и тех аспектов Национальной киберстратегии, которые относятся к содействию росту, инновациям и подготовке квалифицированных кадров. Министр цифровизации возглавляет работу правительства по укреплению британской кибернетической экосистемы и лидерства в сфере технологий, имеющих критическое значение для нашей кибермощи.

- **Министры всех ведущих государственных департаментов, в ведении которых находятся объекты критической национальной инфраструктуры,** отвечают за осуществление политики кибербезопасности и устойчивости в своих секторах.

- **Все министры** должны обеспечивать контроль за кибербезопасностью в своих департаментах и применением надлежащих мер снижения риска. В случаях, когда в ведении какого-либо департамента находится один из элементов государственного или частного сектора (например, министерство выравнивания возможностей, жилищно-коммунального хозяйства и общин (DLUHC) и местные органы власти или министерство охраны окружающей среды, продовольствия и сельского хозяйства (DEFRA) и предприятия водоснабжения), он отвечает за соблюдение политики кибербезопасности и принятие соответствующих мер в этом секторе.

193. На заместителя советника по национальной безопасности по вопросам разведки, безопасности и устойчивости возложена ответственность за реализацию этой стратегии, и он будет возглавлять официальную деятельность по ее реализации в масштабах всего правительства при поддержке соответствующих руководящих лиц в каждом департаменте.

Обязанности министров



* обеспечивает общее руководство в масштабе всех ведомств, гарантируя эффективное реагирование правительства на киберугрозы и достижение наших амбициозных целей как кибердержавы.

Инвестиции в кибермощь

194. В течение следующих 3 лет правительство вложит 2,6 млрд фунтов стерлингов в киберпотенциал и замену устаревших ИТ-систем. Это в дополнение к крупным инвестициям в Национальные силы кибербезопасности. Сюда входят дополнительные инвестиции в сумме 114 млн фунтов стерлингов в Программу укрепления национальной кибербезопасности, при этом ежегодные расходы на наращивание потенциала, предусмотренные стратегией 2016 года, передаются в ведение министерств и переводятся на постоянную основу. Международные программы, направленные на помощь партнерским странам в укреплении их киберустойчивости и способности противостоять киберугрозам, будут осуществляться при поддержке Фонда предотвращения конфликтов, содействия стабильности и безопасности (CSSF). Это наряду с анонсированным увеличением инвестиций в НИОКР, разведку, оборону, инновации, инфраструктуру и квалифицированные кадры, которые будут в той или иной мере способствовать наращиванию кибермощи Соединенного Королевства.[37]

Измерение успеха

195. Реализация стратегии будет основываться на постоянно совершенствующемся механизме оценки результатов, которые будут доводиться до сведения старших ответственных руководителей и персонала Совета национальной безопасности. Этот механизм будет использоваться при подготовке материалов для обсуждения в парламенте и других органах, которые осуществляют контроль за деятельностью органов национальной безопасности. В соответствии с подходом, изложенным в Стратегии национальной кибербезопасности 2016–2021 гг., этот документ не будет находиться в открытом доступе в силу секретного характера содержащейся в нем информации, однако правительство будет публиковать годовые отчеты о достигнутом прогрессе.

196. Механизм оценки результатов поможет:

- определить четкое направление деятельности для достижения различных целей, описанных в стратегии;
- установить ответственность за реализацию стратегии;
- обеспечить транспарентность в отношении достижения страной целей, изложенных в стратегии;
- продемонстрировать, что необходимо сделать, чтобы привести осуществляемую деятельность в соответствие со стратегией;
- понять, какие действия являются эффективными в контексте достижения стратегических целей, чтобы обеспечить применение этого опыта в будущем;
- создать целостное представление о деятельности по достижению всех пяти основополагающих целей, чтобы избежать дублирования и определять сильные и слабые стороны в киберпотенциале страны;
- обеспечить использование стратегии для содействия укреплению кибербезопасности во всех сегментах общества.

[37] HM Treasury, Autumn Budget and Spending Review 2021 (2021)

Следующие шаги

197. Эта стратегия призвана служить руководством к действию не только для тех лиц в правительстве, которые отвечают за политику кибербезопасности и широкий ряд других политических документов в смежных областях (см. Приложение A), но и для каждого человека и организации в масштабах всего общества, которые заинтересованы в поддержке национальных усилий по обеспечению кибербезопасности и отвечают за них. Кроме того, это положило начало дискуссии — которую мы обязательно продолжим — о том, как обеспечить сохранение актуальности наших целей и приоритетов в течение следующих пяти – десяти лет. Мы используем публикацию этой стратегии в качестве платформы для дальнейшего взаимодействия с общественностью, представителями частного и третьего секторов в масштабе всего Соединенного Королевства, и будем рады получить прямую обратную связь на адрес электронной почты ukcyberstrategy@cabinetoffice.gov.uk. Мы будем ежегодно предоставлять отчетность о прогрессе в реализации этой стратегии.

Приложение A. Кибербезопасность в общей повестке дня правительства

Национальная киберстратегия призвана поддерживать и дополнять целый ряд других приоритетов повестки дня правительства в области безопасности, обороны, внешней политики и экономики. В свою очередь, успех этой стратегии опирается на более широкий круг возможностей, разрабатываемых в рамках системы образования и подготовки квалифицированных кадров, и на национальный подход к цифровой, технологической и промышленной политике, исследованиям и развитию бизнеса. В число соответствующих ключевых стратегий и планов входят следующие:

- **Интегрированный обзор**, включая национальные усилия по повышению устойчивости, противодействию государственным угрозам и борьбе с серьезной организованной преступностью и терроризмом, сохранению стратегического преимущества на основе научно-технического прогресса и формированию международного порядка

- **Национальная стратегия в области данных**, излагающая наше видение в отношении возможностей, которые ответственное использование данных обеспечивает для повышения производительности, создания новых компаний и рабочих мест, оптимизации государственных услуг, укрепления более справедливого общества и стимулирования научных открытий, позиционируя Соединенное Королевство в качестве предвестника следующей волны инноваций. Сюда входит преобразование методов использования правительством данных в целях повышения эффективности и качества государственных услуг путем устранения препятствий для обмена данными между департаментами и повышения качества данных, которыми они располагают. Это будет иметь решающее значение для продвижения нашей повестки дня в области кибербезопасности, обеспечивая, например, возможности для сбора и использования качественных данных о киберинцидентах.

- **План стимулирования роста,** помогающий нам **восстановить экономику лучше, чем было,** благодаря дополнительной поддержке и инвестициям в инфраструктуру, подготовку квалифицированных кадров и инновации, а также **Стратегия инноваций**, в которой изложены наши цели по развитию экономики на основе инноваций.

- **План регулирования цифровой среды**, описывающий ориентированный на развитие инноваций подход к регулированию цифровых технологий, который будет стимулировать процветание и укреплять доверие к их использованию.

- **Национальная стратегия развития искусственного интеллекта**, призванная подготовить Соединенное Королевство к наступающему десятилетию преобразований в ИИ путем вложения средств в долгосрочные потребности экосистемы ИИ, поддержки перехода к использованию ИИ в экономике и обеспечения правильной организации управления ИИ-технологиями на внутреннем и международном уровнях. Кроме того, сюда входят меры, направленные на поддержку защищенных от киберугроз инноваций в системы с элементами ИИ, а также на защиту населения и укрепление доверия к использованию ИИ.

- Готовящаяся **Стратегия национальной устойчивости**, в которой, помимо прочего, описывается, как Соединенное Королевство будет отслеживать развитие технологических угроз и сохранять устойчивость в киберпространстве.

- Готовящаяся **Стратегия развития цифровых технологий**, в которой будет четко описано видение целей правительства по использованию интереса к цифровой трансформации, ускорению роста и дальнейшему развитию более инклюзивной, конкурентоспособной и инновационной цифровой экономики в интересах будущего; а также будут определены цели правительства в цифровом секторе на основе Десяти технических приоритетов Министерства цифровизации, культуры, СМИ и спорта.

- **Стратегия по достижению чистого нулевого уровня выбросов,** призванная обеспечить низкоуглеродное будущее нашей процветающей и ориентированной на инновации экономики.

- **План борьбы с преступностью**, в котором описываются меры по восстановлению доверия к системе уголовного правосудия и по претворению в жизнь нашего общего видения — более безопасная Британия, где будет меньше преступлений и меньше жертв.[38]

[38] Министерство внутренних дел, Beating Crime Plan (2021)

Реализацию Национальной киберстратегии непосредственно поддерживают еще две публикации, описывающие пути осуществления отдельных положений стратегии.

- Готовящаяся **Стратегия правительства в области кибербезопасности**, в которой будут изложены более подробные планы по повышению безопасности правительства и государственного сектора, поддерживающие реализацию данной стратегии.
- Готовящийся **Обзор механизмов стимулирования и регулирования 2021 года**, в котором будут изложены результаты оценки эффективности нашей деятельности по стимулированию улучшений в области кибербезопасности во всех секторах экономики и наши предложения по осуществлению коммерческих и организационных элементов основополагающей цели по устойчивости.

Приложение B. Положения NIS – национальная стратегия

Введение

Национальная стратегия NIS

1. Национальная киберстратегия объявлена британской национальной стратегией для целей Положения 2 Британских Положений 2018 года о сетях и информационных системах (NIS).

2. В это приложение включена дополнительная информация, в том числе:

- описание ролей и обязанностей основных органов власти, отвечающих за реализацию Положений NIS в Соединенном Королевстве;
- список основных органов власти, в ведении которых находится эти вопросы.

Британские Положения NIS

3. В 2016 году Европейская Комиссия согласовала Директиву, направленную на повышение безопасности сетей и информационных систем в Европейском Союзе (ЕС). Правительство Соединенного Королевства поддержало эту директиву.

4. 20 апреля 2018 года правительство представило на рассмотрение в парламенте новый документ — Положения 2018 года о сетях и информационных системах (NIS). Эти Положения вступили в силу 10 мая 2018 года.

5. Положениями NIS в Соединенном Королевстве установлен новый режим регулирования, согласно которому назначенные операторы жизненно важных услуг (ОЖВУ) и соответствующие поставщики цифровых услуг (СПЦУ) обязаны принимать технические и организационные меры для обеспечения безопасности своих сетей и информационных систем.

6. Эти Положения действуют в секторах, которые имеют жизненно важное значение для экономики и общества и в значительной степени зависят от работы сетей и информационных систем — энергетика, транспорт, поставка питьевой воды, здравоохранение и цифровая инфраструктура.

7. Сюда также входят ключевые поставщики цифровых услуг (поисковые системы, услуги облачных вычислений и маркетплейсы).

8. Положения NIS устанавливают:

- **национальную организационную структуру,** поддерживающую осуществление положений, включая национальную стратегию;
- отраслевые **компетентные органы**, выполняющие обязанности регулирующих органов;
- Национальный центр кибербезопасности (NCSC), выступающий в роли **единого контактного центра** (SPOC), и **группы по реагированию на инциденты в области компьютерной безопасности** (CSIRT).

9. Оценка прогресса в виде обзоров итогов имплементации выполняется раз в 2–5 лет.

Основные роли и обязанности

Национальная организационная структура

10. Кабинет министров отвечает за национальную киберстратегию, которая включает в себя Национальную стратегию NIS. Кроме того, на Кабинет министров возложена общая ответственность за повышение безопасности и устойчивости критической национальной инфраструктуры.

11. Министерство цифровизации, культуры, СМИ и спорта (DCMS) отвечает за осуществление положений NIS в целом, включая координацию деятельности соответствующих органов и NCSC. Министерство издает инструкции для компетентных органов по поддержке осуществления Положений NIS в масштабах Соединенного Королевства.

Единый контактный центр (ЕКЦ)

12. Национальный контактный центр по взаимодействию с международными [ЕС] партнерами в области NIS осуществляет координацию процесса подачи просьб о принятии мер или о предоставлении информации, а также подает годовую статистическую отчетность об инцидентах. Британским ЕКЦ является Национальный центр кибербезопасности.

Группа по реагированию на инциденты в области компьютерной безопасности (CSIRT)

13. Роль Группы по реагированию на инциденты в области компьютерной безопасности в Соединенном Королевстве выполняет Национальный центр кибербезопасности. Он отвечает за мониторинг инцидентов, связанных с нарушением кибербезопасности, на национальном уровне; обеспечивая анализ угроз в реальном режиме времени, защиту от кибератак на национальные объекты, предоставление технических рекомендаций и реагирование на серьезные киберинциденты, помогая свести ущерб к минимуму.

14. NCSC обеспечивает работу Механизма оценки киберрисков (CAF), ориентированного на достижение результатов, и издает всеобъемлющие рекомендации по вопросам кибербезопасности, выступая в качестве Национального технического эксперта.

Компетентные органы

15. Эти органы отвечают за надзор за осуществлением и обеспечение соблюдения Положений NIS в своих секторах, назначая ОЖВУ и СПЦУ и оценивая соблюдение ими требований, предусмотренных Положениями NIS. Они описаны в Приложении 1 к Положениям NIS; их перечень представлен в разделе 3.

Операторы жизненно важных услуг (ОЖВУ) и соответствующие поставщики цифровых услуг (СПЦУ)

16. ОЖВУ или СПЦУ, которые отвечают пороговым стандартам назначения в соответствующем секторе или были назначены соответствующим органом согласно Положению 8(3) Положений NIS, обязаны соблюдать требования, предусмотренные Положениями NIS.

17. Среди них:

- применение надлежащих и соразмерных технических и организационных мер по управлению рисками для безопасности сети и информационных систем;
- применение надлежащих и соразмерных мер по предотвращению и смягчению последствий инцидентов, нарушающих безопасность сети и информационных систем;
- уведомление соответствующих компетентных органов об инцидентах, оказавших существенное воздействие на предоставляемые ими услуги;
- удовлетворение инспекционных требований согласно Положениям NIS;
- соблюдение требований, содержащихся в уведомлениях о затребовании информации, принудительном исполнении и штрафах.
- СПЦУ также должны быть зарегистрированы в Офисе уполномоченного по информации (ICO)

Другие компетентные органы:

18. В области осуществления Положений NIS правительство Соединенного Королевства тесно сотрудничает с автономными администрациями и другими компетентными органами, включая ведущие министерства.

19. Центр защиты национальной инфраструктуры (CPNI) предоставляет рекомендации по смежным вопросам безопасности физических объектов и персонала.

Перечень ключевых органов, в ведомстве которых находится осуществление Положений NIS

Национальные органы	
Британские Положения NIS	Министерство цифровизации, культуры, СМИ и спорта
Национальная киберстратегия Соединенного Королевства	Кабинет министров
Единый контактный центр (ЕКЦ) Соединенного Королевства	Национальный центр кибербезопасности
Британская Группа по реагированию на инциденты в области компьютерной безопасности (CSIRT)	Национальный центр кибербезопасности

Компетентные органы					
Сектор	**Подсектор**	**Англия**	**Уэльс**	**Шотландия**	**Северная Ирландия**
Энергетика	Электро-энергетика	Совместно: Министерство бизнеса, энергетики и промышленной стратегии и Управление рынками газа и электроэнергии (Ofgem)			Министерство финансов
	Нефть	Министерство бизнеса, энергетики и промышленной стратегии			Министерство финансов
	Газ	Совместно: Министерство бизнеса, энергетики и промышленной стратегии и Управление рынками газа и электроэнергии (Ofgem)[39]			Министерство финансов
Транспорт	Авиация	Совместно: Министерство транспорта и Управление гражданской авиации (CAA)			
	Железная дорога	Министерство транспорта			Министерство финансов
	Водное хозяйство	Министерство транспорта			
	Дороги	Министерство транспорта		Министры Шотландии	Министерство финансов
Здраво-охранение	Медицинские учреждения	Министерство здравоохранения и социальной защиты	Министры Уэльса	Министры Шотландии	Министерство финансов
Питьевая вода	Питьевая вода	Министерство охраны окружающей среды, продовольствия и сельского хозяйства	Министры Уэльса	Управление по контролю за качеством питьевой воды в Шотландии	Министерство финансов
Цифровая инфраструктура	Цифровая инфраструктура	Управление по делам радио, телевидения и предприятий связи (Ofcom)			

[39] В исключительных случаях Министерство бизнеса, энергетики и промышленной стратегии является единственным компетентным органом. Подробную информацию см. в Приложениях 1 и 2 Положений 2018 года о сетях и информационных системах.

Приложение C. Глоссарий

Action Fraud — центр сбора информации о мошенничестве и киберпреступлениях, в который граждане и организации сообщают о случаях, когда они стали жертвами обмана, мошенничества или киберпреступлений в Англии, Уэльсе и Северной Ирландии. В Шотландии о таких случаях следует сообщать в Службу полиции Шотландии.

COBR – брифинг-залы кабинета министров. Физическим центром деятельности британского правительства по реагированию на чрезвычайные ситуации являются брифинг-залы COBR, которые находятся как правило, в Вестминстере и откуда осуществляется централизованное принятие, мониторинг и координация мер реагирования. Он выполняет роль правительственного координационного центра реагирования и служит авторитетным источником рекомендаций для местных служб реагирования.

Crypt-Key (CK) — термин, используемый для описания того, как Соединенное Королевство использует криптографию для защиты критической информации и услуг, от которых зависит работа британского правительства, военных сил и органов национальной безопасности, в том числе защиты от атак со стороны наиболее способных противников.

Cyber Security Body of Knowledge (CyBOK) — уникальный ресурс, в рамках которого впервые предоставляется доступ к совокупности обширных и глубоких знаний, лежащих в основе кибербезопасности и накопленных в широком ряде дисциплин.

GCHQ — Центр правительственной связи, который отвечает за ведение радиоэлектронной разведки и выступает в роли Национального технического эксперта по кибертехнологиям (NTA).

GFCE – Глобальный форум по киберэкспертизе.

ICANN — Корпорация по управлению доменными именами и IP-адресами. Она занимается координацией вопросов, связанных с названиями веб-сайтов и IP-адерсами.

NCA — Национальное агентство по борьбе с преступностью

«Пять глаз» — это разведывательный альянс между США, Соединенным Королевством, Канадой, Австралией и Новой Зеландией, который способствует обмену информацией в целях обеспечения как можно более эффективной защиты их граждан от угроз.

«Умный город» — сообщество, использующее интеграцию информационных и коммуникационных технологий и Интернета вещей для сбора и анализа данных для целей предоставления новых услуг в урбанизированной среде и повышения качества жизни граждан.

Автономная система — система IP-сетей, маршрутизация которых управляется определенной сущностью или доменом.

Автономное правительство или автономная администрация — отдельные органы законодательной и исполнительной власти в Шотландии, Уэльсе и Северной Ирландии, которые были созданы в результате деволюции и отвечают за многие вопросы внутренней политики, пользуясь правом принимать законы в этих областях.

Активная киберзащита (АКЗ) помогает организациям обнаруживать и устранять уязвимости, управлять инцидентами и автоматически останавливать кибератаки. Некоторые сервисы предназначены, главным образом, для государственного сектора, тогда как к другим — в зависимости от их применимости и жизнеспособности — может быть предоставлен доступ более широкому кругу предприятий частного сектора и гражданам.

Аутентификация — процедура проверки подлинности личности или других атрибутов пользователя, процесса или устройства.

Безопасные по дизайну — программное обеспечение, оборудование и системы, которые изначально проектируются из расчета на безопасность.

Домен — доменное имя служит для указания местонахождения организации или иного объекта в интернете и соответствует сетевому адресу в интернете (IP-адресу).

Интегрированный обзор «Глобальная Британия в эпоху соперничества» — комплексный обзор политики в области безопасности, обороны, развития и иностранных дел, описывающий, как правительство видит роль, которую Соединенное Королевство будет играть в мире в течение следующего десятилетия и деятельность, которую правительство осуществит к 2025 году.

Интернет вещей — совокупность устройств, транспортных средств, зданий и других объектов со встроенной электроникой, программным обеспечением и сенсорами, которые сообщаются и обмениваются данными через интернет.

Интернет — всемирная компьютерная сеть, включающая разнообразные информационно-коммуникационные объекты, состоящие из взаимосвязанных сетей, использующих стандартизированные протоколы передачи данных.

Искусственный интеллект — технология, позволяющая программировать компьютерные системы «думать самостоятельно», автономно адаптируясь и работая. ИИ находит все более широкое применение в решении более сложных задач, таких как медицинская диагностика, изыскание новых лекарственных средств и прогнозное техническое обслуживание.

Квантовые технологии — технологии, основанные на принципах квантовой физики. Углубление понимания так называемых «квантовых эффектов», таких как суперпозиция и запутанность, а также управление ими, приведет к новой волне достижений, которые составят основу нашей экономики и общества, в области зондирования, передачи данных, криптографии, измерения времени и вычислений.

Кибератака — умышленное использование компьютерных систем, предприятий, деятельность которых зависит от цифровых технологий, и сетей с целью причинения вреда.

Кибербезопасность — защита подключенных к интернету систем (в том числе оборудования, программного обеспечения и связанной с ними инфраструктуры), данных на них и услуг, которые они предоставляют, от несанкционированного доступа, повреждения или злоупотребления. Сюда входит ущерб, нанесенный оператором системы умышленно или случайно в результате несоблюдения режима безопасности или под воздействием других лиц.

Киберинцидент — происшествие, представляющее или способное представлять угрозу компьютеру, подключенному к интернету устройству или сети (или данным, которые обрабатываются, хранятся в этих системах или передаются между ними), для смягчения последствий которого может потребоваться применение мер реагирования.

Кибернетическая экосистема — совокупность взаимосвязанных объектов инфраструктуры, лиц, процессов, данных, информационно-коммуникационных технологий, а также среды и условий, влияющих на их взаимодействие.

Киберпреступления — кибер-зависимые преступления (преступления, которые можно совершить только с использованием устройств ИКТ, причем эти устройства являются как орудием, так и объектом преступления), или преступления с киберсоставляющей (преступления, которые можно совершить и без использования устройств ИКТ, например финансовое мошенничество, но масштаб и охват которых существенно увеличивается за счет использования ИКТ).

Киберриск — потенциальная возможность использования уязвимостей информационной системы конкретной угрозой для причинения ущерба организации.

Киберугроза — все, что может нарушить безопасность и целостность информационных систем и подключенных к интернету устройств (в том числе оборудования, программного обеспечения и связанной с ними инфраструктуры), данных на них и услуг, которые они предоставляют, преимущественно с использованием киберпространства.

Киберустойчивость — общая способность систем, организаций и граждан выдерживать кибератаки и — в случае их успеха — восстанавливаться.

Компетентные органы — регулирующие органы, перечисленные в Положениях 2018 года о сетях и информационных системах (NIS). Есть целый ряд компетентных органов, которые отвечают за вопросы NIS в разных секторах.

Криптовалюта — цифровая валютная и платежная система, например биткойн.

Криптография — наука о методах анализа и дешифровки кодов и шифров, криптоанализ.

Критическая национальная инфраструктура — критически важные элементы инфраструктуры (активы, объекты, системы, сети или процессы, а также работники особо важной категории, занимающиеся их эксплуатацией или поддержкой), потеря или нарушение безопасности которых могут привести к:

а) значительным пагубным последствиям для доступности, целостности или предоставления жизненно важных услуг, в том числе услуг, нарушение целостности которых может привести к гибели или телесному повреждению многих людей, учитывая их серьезные последствия в экономическом или социальном плане; и/или

б) серьезным последствиям для национальной безопасности, национальной обороны или для функционирования государства.

Механизм оценки киберрисков (CAF) предлагает систематический и комплексный подход к оценке степени, до которой организации, которые отвечают за жизненно важные функции, обеспечивают управление своими киберрисками.

Микрогенерация — мелкомасштабное производство электроэнергии домохозяйствами, небольшими компаниям и сообществами.

Наступательные кибероперации — добавление, удаление данных или манипулирование данными в системах или сетях в целях достижения физического, виртуального или когнитивного эффекта. Наступательные кибероперации часто основаны на использовании технических уязвимостей, систем или сетей способами, не предусмотренными или не одобряемыми их операторами, и могут опираться на обман и введение в заблуждение.

НАТО — Организация Североатлантического договора.

Национальный центр кибербезопасности (NCSC) — технический орган, отвечающий за вопросы, связанные с киберугрозами, который обеспечивает единый национальный подход к реагированию на киберинциденты в целях снижения ущерба, помогая пострадавшим восстанавливаться и извлекать уроки на будущее.

Операторы жизненно важных услуг — организации в жизненно важных секторах, работа которых в значительной степени зависит от информационных сетей, как например предприятия в секторах коммунальных услуг, здравоохранения, транспорта и цифровой инфраструктуры, отвечающие критериям, установленным Положениями 2018 года о сетях и информационных системах (NIS).

Операционные технологии (OT) сочетают в себе аппаратное и программное обеспечение, обеспечивая мониторинг, контроль и автоматизацию физических процессов, прежде всего в промышленных секторах, таких как энергетика, производство, водное хозяйство и транспорт.

ОЭСР — Организация экономического сотрудничества и развития, межправительственная экономическая организация.

План регулирования цифровой среды излагает общий подход правительства к регулированию цифровых технологий в целях содействия росту и инновациям.

Положения 2018 года о сетях и информационных системах (NIS) предусматривают правовые меры, направленные на повышение уровня безопасности (как кибер-, так и физическую устойчивость) сетей и информационных систем, использующихся для предоставления жизненно важных и цифровых услуг.

Поставщики управляемых услуг — сторонние компании, которые предоставляют определенные услуги для клиентов и отвечают за их работу, обслуживание и безопасность.

Правительственный координационный центр кибербезопасности (GCCC) — перспективный совместный проект GSG, CDDO и NCSC, направленный на объединение функциональных обязанностей, опыта и знаний, накопленных этими организациями, для целей обеспечения более эффективной координации оперативных усилий в области кибербезопасности в масштабах всего правительства, оптимизации использования информации о безопасности и разведывательных данных об угрозах в масштабах всего правительства и реального улучшения способности правительства обеспечить «единую оборону».

Программа-вымогатель — вредоносное программное обеспечение, которое лишает пользователя доступа к его файлам, компьютеру или устройству до тех пор, пока не будет выплачен выкуп.

Промышленная система управления (ПСУ) — информационная система, используемая для управления промышленными процессами, такими как изготовление, обработка продуктов, производство и дистрибуция, или для контроля инфраструктурных активов.

Реагирование на инцидент — деятельность по устранению непосредственных последствий происшествия в краткосрочной перспективе, а также возможность применения временных мер по восстановлению после него.

Сканирование горизонтов — систематическое изучение информации в целях определения потенциальных угроз, рисков, появляющихся проблем и возможностей, что позволяет лучше подготовиться к ним и предусматривать меры по их смягчению и использованию в процессе формирования политики.

Служба уведомлений об уязвимостях — механизм, с помощью которого организации могут получать оповещения о брешах в системе безопасности до того, как ими могут воспользоваться злоумышленники.

Технология блокчейн — это особый способ хранения данных. Блокчейн — это разновидность распределённого реестра, то есть технологии хранения данных, предназначенной только для добавления информации и защищенной от несанкционированного доступа.

Унаследованные ИТ-системы — это системы и их компонентное программное обеспечение и аппаратные средства, для которых недоступна поддержка поставщика или требуется расширенная поддержка и/или поддержка согласно индивидуальной договоренности

Управление инцидентами — организация и координация деятельности по расследованию фактического или потенциального случая враждебной кибератаки, который мог причинить или причинил вред системе или сети, и восстановлению после него.

Утечка данных — несанкционированная передача или раскрытие информации, хранящейся в сети, стороне, которая не имеет права доступа к ней.

Уязвимость — ошибки в программном обеспечении, которые могут быть использованы злоумышленниками.

Целостность в контексте информационной безопасности означает, что информация не была случайно или умышленно изменена и является точной и полной.

Цифровые двойники — виртуальные копии или представления физических объектов, процессов, систем или организаций в урбанизированной, социальной или природной среде, которые позволяют проанализировать поведение комплексных физических объектов и граждан, помогая организациям принимать более эффективные решения и оптимизировать процессы. Изменения в реальном мире отражаются в цифровом двойнике, а изменения в цифровом двойнике могут быть автоматически воспроизведены в реальном мире.