HM Government

НАЦИОНАЛЬНАЯ СТРАТЕГИЯ КИБЕРБЕЗОПАСНОСТИ 2016–2021

Содержание

ПРЕДИСЛОВИЕ

Великобритания входит в число лидеров в области цифровых технологий. В значительной мере наше благосостояние зависит от способности защитить технологии, данные и сети от множества стоящих перед нами угроз.

При этом кибератаки становятся более массовыми, изощренными и имеют разрушительные последствия в случае успешного осуществления. Поэтому мы принимаем решительные меры для защиты нашей экономики и неприкосновенности частной жизни граждан Великобритании.

В Национальной стратегии кибербезопасности изложен план по превращению Великобритании в государство, способное уверенно противостоять угрозам в условиях быстрого развития цифровых технологий.

На протяжении пятилетнего периода действия стратегии мы вложим 1,9 млрд фунтов в защиту систем и инфраструктуры, сдерживание противников и наращивание соответствующего потенциала в масштабах всего общества — от крупнейших компаний до отдельных граждан.

Нам требуется комплексный подход к кибербезопасности, начиная с элементарных правил безопасности и заканчивая самыми изощренными методами сдерживания угроз.

Мы направим усилия на то, чтобы атаки на какие бы то ни было объекты в Великобритании дорого обходились злоумышленникам. С этой целью мы будем как укреплять оборону, так и развивать кадровый потенциал в области кибернетики. Этот вопрос уже вышел за рамки ИТ-департаментов и касается каждого сотрудника. Навыки кибербезопасности должны войти в должностные обязанности каждой профессии.

Национальный центр кибербезопасности станет центром мирового класса, предоставляющим удобный доступ к передовым знаниям и опыту для бизнеса и отдельных граждан, а также обеспечивающим оперативное реагирование на крупные происшествия.

Правительству, определенно, отводится роль лидера, но в то же время мы будем способствовать развитию широкой коммерческой экосистемы, признавая, что в определенных сферах бизнес способен быстрее внедрять инновации. Сюда же входят планы по привлечению самой талантливой молодежи к работе в области кибербезопасности.

Киберугрозы затрагивают наше общество в целом, поэтому мы считаем, что каждый член общества обязан вносить свой вклад в общее дело национального противодействия. Именно поэтому настоящая стратегия является беспрецедентной по своей прозрачности. Мы больше не можем позволить себе обсуждать эти вопросы за закрытой дверью.

В конечном итоге, речь идет об угрозе, которую невозможно ликвидировать полностью. Цифровые технологии успешно работают, потому что являются открытыми, а открытость сопряжена с риском. Однако нам под силу сократить эту угрозу до уровня, при котором мы можем оставаться в авангарде цифровой революции. В настоящей стратегии изложено, как этого добиться.

Достопочтенный Филип Хэммонд, член парламента, Министр финансов Великобритании

ВСТУПЛЕНИЕ

Наши главные обязанности — обеспечить безопасность государства и компетентное управление им. Эти обязанности отражены в настоящей стратегии. Она представляет собой смелый и масштабный подход к противостоянию многочисленным угрозам, стоящим перед нашим государством в киберпространстве. Устранение и смягчение этих угроз — наша общая задача, однако правительство понимает, что оно должно возглавить деятельность государства в этой области.

Правительство твердо намерено обеспечить выполнение обязательств, изложенных в настоящей стратегии, а также надлежащий мониторинг и регулярную отчетность о прогрессе в их выполнении. Мы также будем постоянно пересматривать наши подходы с учетом изменения уровня угроз, стоящих перед нами, а также достижений технологий безопасности.

Правительство также несет особую ответственность перед гражданами, компаниями и организациями, работающими в Великобритании, а также международными союзниками и партнерами. У нас должна быть возможность заверить их в том, что мы делаем все возможное для сохранения безопасности систем и защиты данных и сетей от атак или вмешательства. Именно поэтому мы должны установить для себя самые высокие стандарты кибербезопасности и неуклонно их соблюдать, чтобы, с одной стороны, продемонстрировать их важность для национальной безопасности, а с другой, — служить примером для подражания. Мы будем отчитываться о достигнутом прогрессе на ежегодной основе.

Как член Кабинета министров, который отвечает за кибербезопасность и безопасность правительства, я твердо намерен содействовать полной реализации этой стратегии. Я буду тесно сотрудничать с коллегами по Правительству, партнерами из Правительств Шотландии, Уэльса и Северной Ирландии, а также с организациями государственного сектора в целом, бизнесом и научными организациями, чтобы обеспечить достижение этой цели.

Достопочтенный Бен Гаммер, член парламента,
Министр Кабинета министров и начальник казначейства

1 КРАТКОЕ СОДЕРЖАНИЕ

1.1. Будущая безопасность и процветание Великобритании зиждется на цифровых технологиях. Перед нашим поколением стоит задача построения процветающего цифрового общества, которое, с одной стороны, является устойчивым к киберугрозам, а с другой стороны — обладает знаниями и потенциалом, необходимыми для максимально эффективного использования возможностей и управления рисками.

1.2. Мы находимся в критической зависимости от интернета. Однако он по своей природе является небезопасным, и неизбежно будут попытки использовать его уязвимости для кибератак. Устранить эту угрозу полностью невозможно, но риск ее можно существенно сократить до уровня, при котором возможно дальнейшее процветание общества и получение выгод от огромных возможностей, которые дают цифровые технологии.

1.3. Национальная стратегия кибербезопасности 2011 года, в основу которой легла Национальная программа кибербезопасности стоимостью 860 млн фунтов, обеспечила существенное повышение кибербезопасности Великобритании. Важные результаты были достигнуты за счет стимулирования рынком безопасного поведения в киберпространстве. Однако этот подход не обеспечил масштаба и темпов перемен, необходимых для того, чтобы опережать быстро развивающиеся угрозы. Мы должны пойти еще дальше.

1.4. Согласно нашему видению, к 2021 году в **Великобритании будут обеспечены безопасность, устойчивость к киберугрозам, процветание и условия для уверенного пользования цифровыми технологиями**.

1.5. Для претворения этого видения в жизнь мы направим усилия на достижение следующих целей:

• **ОБОРОНА** У нас есть средства для защиты Великобритании от эволюционирующих киберугроз, для эффективного реагирования на происшествия, для защиты британских сетей, данных и систем и повышения их устойчивости к угрозам. Граждане, компании и организации государственного сектора обладают необходимыми знаниями и возможностями для своей защиты.
• **СДЕРЖИВАНИЕ** Великобритания не будет легкой целью для агрессии в киберпространстве в какой бы то ни было форме. Мы способны обнаруживать, понимать, расследовать и срывать попытки враждебных действий, направленных против нас, преследуя и наказывая преступников. У нас есть средства для применения наступательных мер в киберпространстве, если мы сочтем это целесообразным.
• **РАЗВИТИЕ** У нас есть инновационная, развивающаяся индустрия кибербезопасности, опирающаяся на научно-технические достижения и разработки на уровне лучших мировых стандартов. У нас есть самодостаточный кадровый резерв, отвечающий потребностям государственного и частного сектора. Наши передовые аналитические технологии и опыт помогут Великобритании преодолеть будущие угрозы и вызовы.

1.6. В стремлении к достижению этих целей мы будем осуществлять **МЕЖДУНАРОДНУЮ ДЕЯТЕЛЬНОСТЬ** и оказывать влияние путем вкладывания средств в партнерства, формирующие мировое развитие киберпространства таким образом, чтобы продвигать свои интересы в экономике и безопасности в целом. Мы углубим существующие связи с нашими близкими международными партнерами, признавая, что это укрепляет коллективную безопасность. Мы также будем развивать отношения с новыми партнерами, способствуя повышению уровня их кибербезопасности и защите интересов Великобритании за рубежом. Мы будем осуществлять эту деятельность как на двустороннем, так и на многостороннем уровне, в том числе через ЕС, НАТО и ООН. Мы

дадим ясно понять нашим противникам, угрожающим нашим интересам или интересам наших союзников в киберпространстве, какие последствия их ждут.

1.7. Для достижения этих результатов в течение следующих пяти лет Британское правительство намеревается действовать более активно и использовать больше инвестиций, продолжая стимулировать рыночные силы, направленные на повышение стандартов кибербезопасности в масштабах всей Великобритании. Правительство Великобритании в партнерстве с Правительствами Шотландии, Уэльса и Северной Ирландии продолжит сотрудничество с представителями частного и государственного сектора, нацеленное на внедрение правил безопасного поведения в Интернете со стороны граждан, компаний и организаций. Мы разработаем меры, которые будем применять (в случае необходимости и в пределах наших полномочий) для обеспечения улучшений, отвечающих национальным интересам, в частности, если они касаются кибербезопасности критической национальной инфраструктуры.

1.8. Правительство Великобритании, опираясь на свои возможности и возможности отрасли, будет развивать и применять меры активной киберзащиты[1] с целью существенного повышения уровней кибербезопасности в масштабах всех британских сетей. В число этих мер входит сведение к минимуму самых распространенных форм фишинга, фильтрация известных атакующих IP-адресов и активное блокирование вредоносной деятельности в интернете. Улучшение мер элементарной киберзащиты позволит укрепить устойчивость Великобритании к самым распространенным киберугрозам.

1.9. Мы основали Национальный центр киберзащиты (NCSC) как орган, отвечающий за киберзащиту в Великобритании, обмен знаниями, устранение системных уязвимостей и руководство ключевой деятельностью в области национальной кибербезопасности.

1.10. Мы обязуемся обеспечить, чтобы наши Вооруженные силы были устойчивыми к угрозам кибербезопасности, имели необходимые средства для киберзащиты своих сетей и платформ, были способны продолжать свои операции и сохранили глобальную свободу маневрирования, невзирая на киберугрозы. Военный Центр операций по кибербезопасности будет тесно сотрудничать с NCSC и обеспечит необходимую поддержку со стороны Вооруженных сил в случае крупной кибератаки на государство.

1.11. У нас будут средства, необходимые для реагирования на кибератаки так же, как мы реагируем на любые другие атаки, с использованием самых подходящих в той или иной ситуации возможностей, в том числе возможности наступательных кибероопераций.

1.12. Опираясь на авторитет и влияние Британского правительства, мы будем вкладывать средства в программы по устранению дефицита квалифицированных кадров в области кибернетики в Великобритании, начиная со школ и университетов и заканчивая трудовыми ресурсами.

1.13. Мы откроем два новых центра по инновациям в кибернетике, призванных способствовать разработке самых передовых продуктов в этой отрасли и развитию новых, динамичных компаний по кибербезопасности. Мы также выделим часть средств из Фонда обороны и инноваций в кибернетике, объем которого составляет 165 млн фунтов, на закупку инновационных продуктов на нужды обороны и безопасности.

[1] Понимание угроз для безопасности сетей с последующей разработкой и внедрением мер по инициативному противодействию этим угрозам и защите от них. См. объяснение всех технических терминов в Глоссарии.

1.14. В течение следующих пяти лет мы вложим в общей сложности 2,9 млрд фунтов в кардинальную трансформацию системы кибербезопасности Великобритании.

2. ВВЕДЕНИЕ

2.1. За последние два десятилетия информационные и коммуникационные технологии существенно эволюционировали и стали частью нашей жизни практически во всех сферах. Великобритания — общество, с высоким уровнем проникновения цифровых технологий. Это существенно обогатило нашу экономику и повседневную жизнь.

2.2. Трансформация, связанная с повсеместным проникновением цифровых технологий в нашу жизнь, создает новые зависимости. Наша экономика, управление государством и предоставление основных услуг зависят от целостности киберпространства, а также инфраструктуры, систем и данных, лежащих в его основе. Потеря уверенности в этой целостности может поставить под угрозу преимущества технологической революции.

2.3. Значительная часть оборудования и программного обеспечения, изначально разрабатываемого для поддержки этой взаимосвязанной цифровой среды, главным образом ориентирована на аспекты эффективности, стоимости и удобства пользования, но не всегда разрабатывалась из расчета на безопасность с самого начала. Злоумышленники — враждебные государства, преступные или террористические организации и лица — могут эксплуатировать уязвимости, связанные с этим разрывом между удобством и безопасностью. Сокращение этого разрыва является одним из национальных приоритетов.

2.4. С выходом интернета за рамки компьютеров и мобильных телефонов — в другие киберфизические или «умные» системы —опасность удаленного несанкционированного использования распространяется на целый ряд новых технологий. Системы и технологии, лежащие в основе повседневной жизни, такие как электросети, системы управления воздушным движением, спутники, медицинские технологии, промышленные предприятия и светофоры, подключены к интернету и, таким образом, потенциально подвержены опасности несанкционированного вмешательства.

2.5. Национальная стратегия безопасности 2015 г. (NSS) еще раз подтвердила, что угрозы для британских интересов в киберпространстве представляют собой риск первого уровня. В NSS изложено твердое намерение Правительства бороться с киберугрозами и, «будучи мировым лидером в области кибербезопасности, разработать жесткие инновационные меры». Национальная стратегия кибербезопасности принята в рамках выполнения этого обязательства.

2.6. При подготовке этой стратегии Правительство опиралось на достижения, цели и оценки первой пятилетней Национальной стратегии кибербезопасности, принятой в 2011 году. В течение этого периода Правительство инвестировало 860 млн фунтов и гордится достигнутыми результатами. Политика, институты и инициативы, разработанные за последние пять лет, помогли укрепить позиции Великобритании как ведущего глобального игрока в области кибербезопасности.

2.7. Это прочные основы. Однако настойчивость и изобретательность тех, кто может нам угрожать, и существование уязвимостей и недостатков в возможностях и средствах защиты означает, что мы должны активизировать усилия, чтобы идти в ногу с угрозами. Для эффективной защиты наших интересов в киберпространстве требуется комплексный подход. Наше решение по дальнейшему вложению средств и разработке мер основывается на следующих оценках:

- масштаб и динамическая природа киберугроз, равно как и наша уязвимость и зависимость, означают, что текущий подход сам по себе не обеспечивает

достаточного уровня нашей безопасности;
• рыночный подход к продвижению элементарных правил кибербезопасности не обеспечил необходимых темпов и масштаба изменений; поэтому Правительство должно проявить инициативу и принять более активные меры, используя свое влияние и ресурсы для борьбы с киберугрозами;
• Правительство само по себе не в состоянии охватить все аспекты национальной безопасности. Требуется интегрированный и устойчивый подход, предусматривающий привлечение граждан, представителей отрасли и других партнеров в обществе и правительстве к полноценному участию в обеспечении безопасности наших сетей, услуг и данных;
• Великобритании требуется жизнеспособный сектор кибербезопасности и соответствующий кадровый резерв, которые помогут нам идти в ногу с эволюционирующими угрозами и опережать их развитие.

ПРЕДМЕТ СТРАТЕГИИ

2.8. Настоящая стратегия направлена на формирование политики Правительства, а также последовательного и убедительного видения, которое можно представить на суд общественности, бизнеса, гражданского общества, научных организаций и более широких кругов населения.

2.9. Данная стратегия охватывает всю Великобританию. Британское Правительство будет стремиться к обеспечению реализации этой стратегии в масштабах всей Великобритании, признавая при этом, что в той мере, в которой она касается вопросов автономий, мы будем тесно сотрудничать с Правительствами Шотландии, Уэльса и Северной Ирландии в отношении ее применимости к этим территориям (уважая существование в Великобритании трех отдельных правовых юрисдикций и четырех систем образования). В той части, в которой предложения, изложенные в настоящей стратегии, относятся к вопросам автономий, их реализация будет надлежащим образом согласована с соответствующими правительствами согласно соглашениям о деволюции власти.

2.10. В настоящей стратегии изложены предложенные и рекомендованные нами действия, нацеленные на все сектора экономики и общества, начиная с правительственных департаментов и заканчивая ведущими предприятиями и отдельными гражданами. Цель стратегии — повышение кибербезопасности на всех уровнях для общего блага. Она будет служить основой для международной деятельности Великобритании по продвижению надлежащих практик управления интернетом.

2.11. В настоящей стратегии понятие «кибербезопасность» относится к защите информационных систем (оборудования, программного обеспечения и связанной с ними инфраструктуры), содержащихся в них данных и предоставляемых в их рамках услугам от несанкционированного доступа, повреждения и злоупотреблений. Сюда входит урон, нанесенный оператором системы умышленно или случайно в результате несоблюдения режима безопасности.

2.12. В соответствии с оценкой вызовов, стоящих перед нами, и в продолжение достижений стратегии 2011 года, в настоящем документе изложено следующее:

• обновленная оценка стратегического контекста, в том числе текущих и эволюционирующих угроз: кто представляет наибольшую опасность для наших интересов и какие средства есть в их распоряжении;
• обзор уязвимостей и их развития в течение последних пяти лет;
• наше видение кибербезопасности в 2021 году и основные цели на пути его реализации, в том числе руководящие принципы, роли и обязанности, а также описание того, каким образом и в каких областях вмешательство

правительства может оказать положительное влияние;
• пути реализации нашей политики с описанием областей, в которых Правительство должно возглавить работу, и областей, в которых оно будет работать в партнерстве с другими;
• методы оценки прогресса в достижении поставленных целей.

3. СТРАТЕГИЧЕСКИЙ КОНТЕКСТ

3.1. Когда была опубликована предыдущая версия Национальной стратегии кибербезопасности 2011 года, масштаб технологических перемен и их воздействие уже были очевидными. Описанные в ней тенденции и возможности с тех пор усилились. Появились новые технологии и сферы применения, получили более широкое распространение интернет-технологии во всем мире и, в частности, в развивающихся странах, что расширило возможности экономического и социального развития. Все это обеспечило или сможет обеспечить существенные преимущества для таких обществ с высоким уровнем коммуникативных связей, как наше. Однако по мере усиления зависимости Великобритании и других стран от сетей открывается все больше возможностей для нарушения безопасности наших систем и данных. Изменился также и геополитический ландшафт. Вредоносная кибердеятельность не знает международных границ. Игроки государственного масштаба экспериментируют с возможностями ведения наступательных кибероперациий. Киберпреступники расширяют область и стратегические методы преступной деятельности с целью получения большей выгоды от атак на британских граждан, организации и институты. Террористы и симпатизирующие им лица осуществляют атаки низкого уровня и стремятся к осуществлению более серьезных деяний. В данной главе изложена наша оценка характера этих угроз, наших уязвимостей и перспектив их эволюции.

УГРОЗЫ

Киберпреступники

3.2. Настоящая стратегия рассматривает киберпреступность в контексте двух взаимосвязанных форм преступной деятельности:

• кибер-зависимые преступления — преступления, которые можно совершить только с использованием устройств на основе информационно-коммуникационных технологий (ИКТ) и в которых эти устройства являются как орудием, так и целью преступления (т. е. разработка и распространение вредоносных программ с целью финансового обогащения, взлом с целью кражи, повреждения, искажения или уничтожения данных и (или) сети или деятельности),
• преступления с использованием киберпространства — «традиционные» преступления (например, мошенничество или кража данных), масштаб и охват которых можно увеличить за счет использования компьютеров, компьютерных сетей и других форм ИКТ.

3.3. Большую часть наиболее серьезных киберпреступлений против Великобритании (в основном, мошенничество, кража и вымогательство), как и ранее, совершают финансово мотивированные организованные русскоговорящие преступные группировки (ОПГ) в странах Восточной Европы, при этом значительная часть рынка криминальных услуг размещается на компьютерах в этих странах. Однако угрозы исходят из других стран и регионов, а также из самой Великобритании, при этом растущую обеспокоенность вызывает появление угроз из стран Южной Азии и Западной Африки.

3.4. Даже когда удается установить личности главных лиц, причастных к самым разрушительным кибератакам против Великобритании, не часто Великобритании и международным правоохранительным органам удается привлечь их к ответственности, потому что они находятся в юрисдикции стран, с которыми у нас заключены очень ограниченные (или вообще отсутствуют) договоренности об экстрадиции.

3.5. В разработке и развертывании все более совершенных вредоносных программ, заражающих компьютеры и сети британских

граждан, предприятий и правительства, главным образом, виновны эти ОПГ. Воздействие этой деятельности рассеяно по всей Великобритании, но суммарный эффект является существенным. Эти атаки становятся все более агрессивными и вызывающими, о чем свидетельствуют растущие масштабы использования программ-вымогателей и угроз использования распределенных атак типа «отказ в обслуживании» (DDoS) в вымогательских целях.

3.6. Тогда как ОПГ могут представлять значительную угрозу нашему коллективному благосостоянию и безопасности, не меньшую обеспокоенность вызывает угроза, которую представляют менее изощренные, но более распространенные киберпреступления против отдельных лиц и небольших организаций.

Объемы мошенничества в дистанционном банковском обслуживании, включая мошенническое снятие платежей с банковского счета клиента с помощью интернет-банкинга, увеличились на 64% и составили 133,5 млн фунтов в 2015 г. Количество преступлений увеличивалось более медленными темпами (23%), что, по мнению организации Financial Fraud Action UK, говорит о растущей тенденции среди преступников выбирать объекты для атаки среди компаний и состоятельных клиентов.

Исходящие от иностранных государств и спонсируемые государством угрозы

3.7. Мы регулярно наблюдаем попытки со стороны государств и групп, пользующихся государственной поддержкой, проникнуть в британские сети, чтобы получить политические, дипломатические, технологические, коммерческие и стратегические преимущества, прежде всего, в государственном, оборонном, финансовом, энергетическом и телекоммуникационном секторах.

3.8. Объем и воздействие таких государственных кибер-программ может быть различным. Самые технологически развитые государства продолжают стабильно улучшать свои возможности, интегрируя в свои инструментальные средства сервисы шифрования и анонимизации, чтобы скрыть свое вмешательство. Хотя они и имеют в своем распоряжении технические возможности для развертывания изощренных атак, своих целей они зачастую достигают с помощью элементарных инструментов и приемов, пользуясь тем, что уязвимые объекты их преступлений имеют слабую защиту.

3.9. Лишь немногие государства имеют технические возможности для развертывания атак, представляющих серьезную угрозу для безопасности и благосостояния Великобритании в целом. Однако многие другие государства занимаются разработкой изощренных кибер-программ, которые могут представлять угрозу интересам Великобритании в недалеком будущем. Многие государства, стремящиеся расширить свои возможности кибершпионажа, имеют возможность купить инструментальные средства, позволяющие использовать уязвимости сетей, в готовом виде и переориентировать их для шпионажа.

3.10. Помимо средств шпионажа, небольшое число враждебных иностранных злоумышленников, разрабатывают и развертывают возможности наступательных действий в киберпространстве, в том числе разрушительного характера. Это угрожает безопасности критически важной национальной инфраструктуры Великобритании и промышленных систем управления. Некоторые государства используют такие возможности в нарушение международных законов, будучи уверенными в своей относительной безнаказанности и поощряя других следовать их примеру. Хотя разрушительные атаки остаются редким явлением в мире, их количество возрастает и воздействие усиливается.

Террористы

3.11. Террористические группы продолжают вынашивать планы разрушительных кибератак против Великобритании и ее интересов. В настоящее время технические возможности террористов оцениваются как низкие. Тем не менее, воздействие, которое имела их деятельность против Великобритании до настоящего времени, даже такого низкого уровня, было непропорционально высоким: простой дефейс сайтов и доксинг (обнародование раскрытых личных данных в сети) позволили террористическим группам и их сторонникам привлечь внимание СМИ и запугать своих жертв.

«Использование террористами интернета в своих целях не приравнивается к кибертерроризму. Однако можно предположить, что с активизацией их деятельности в киберпространстве и при наличии доступа к киберпреступности как услуге, они могли бы получить возможность осуществления кибератак».

ENISA Threat Landscape 2015

3.12. Согласно текущим оценкам, именно физические террористические атаки, а не кибератаки, будут оставаться приоритетом для террористических групп в ближайшем будущем. Мы полагаем, что с подключением к экстремистской деятельности компьютерно-грамотного поколения и появлением возможности обмена продвинутыми техническими умениями, можно ожидать увеличения объема не особенно изощренной деятельности против Великобритании (дефейс или DDoS-атаки). Кроме того, повышается вероятность появления ряда квалифицированных экстремистов-одиночек, равно как и риск того, что террористические организации будут пытаться завербовать инсайдеров из числа давно работающих в организации сотрудников. Весьма вероятно, что террористы будут обращаться к любым киберсредствам для достижения максимального эффекта. Таким образом, даже умеренное расширение возможностей террористов может представлять собой существенную угрозу для Великобритании и ее интересов.

Хактивисты

3.13. Группы хактивистов децентрализованы и ориентированы на определенные идеи. Они формируются и выбирают объекты для атак как ответ на то, что вызывает их недовольство, привнося таким образом во многие свои действия элемент «народного мщения». Тогда как большая часть кибердеятельности хактивистов является дезорганизующей по своей природе (дефейс веб-сайтов или атаки DDoS), действия более талантливых из них причинили гораздо более серьезные и длительные последствия для их жертв.

ИНСАЙДЕРЫ

Инсайдерские угрозы продолжают представлять риски для безопасности британских организаций в киберпространстве. Внутренние злоумышленники, которые пользуются доверием в своих организациях и имеют доступ к критически важным системам и данным, представляют самую большую угрозу. Они способны причинить финансовый урон и подорвать репутацию в результате кражи секретных данных и объектов интеллектуальной собственности. Они также могут составлять угрозу деструктивной кибердеятельности, если воспользуются особыми знаниями или доступом для осуществления атаки или содействия ей с целью вывода из строя или ухудшения критически важных услуг в сети их организации или уничтожения данных.

Не меньшую обеспокоенность вызывают и те инсайдеры или сотрудники, которые могут случайно нанести урон организации, если неумышленно перейдут по ссылке в фишинговом сообщении, вставят в компьютер USB-накопитель, зараженный вирусом, или пренебрегут правилами безопасности и загрузят небезопасное содержимое из сети. И хотя у них нет намерения умышленно навредить, они способны нанести не менее

существенный урон организации, чем внутренние злоумышленники, в силу того, что обладают особыми правами доступа к системам и данным. Эти лица часто становятся жертвами социальной инженерии, т. е. они могут, сами не сознавая того, предоставить мошенникам доступ к сетям своей организации или выполнить их указания, исходя из лучших побуждений. Общий риск для организации, связанный с инсайдерскими угрозами, касается не только неавторизованного доступа к информационным системам и их содержимому. Не меньшее значение имеют средства физической безопасности, используемые для защиты этих систем от неправомерного доступа или выноса секретных данных или защищенной авторским правом информации, записанных на носителях любого вида. Аналогично, крепкая культура безопасности персонала, способствующая выявлению угроз, которые представляют собой недовольные сотрудники, случаев мошенничества среди персонала, а также промышленного и иного шпионажа является важным элементом комплексного подхода к безопасности.

«Скрипт-кидди»

3.14. По нашим оценкам, так называемые «скрипт-кидди» — как правило, дилетанты, пользующиеся скриптами или программами, разработанными другими, для атаки компьютерных систем и сетей — не представляют серьезной угрозы для экономики или общества. Однако они имеют доступ к хакерским руководствам, ресурсам и инструментам через интернет. В силу уязвимостей систем с выходом в интернет, используемых многими организациями, действия «скрпит-кидди» могут, в некоторых случаях, иметь непропорционально серьезные последствия для пострадавшей организации.

ПРИМЕР ИЗ ПРАКТИКИ 1: КОМПРОМИСС TALKTALK

21 октября 2015 г. британский поставщик услуг связи TalkTalk сообщил об успешной кибератаке на него и возможной утечке клиентских данных. Последующее расследование показало, что доступ к базе данных, содержащей сведения о клиентах, был получен через серверы, имеющие выход в интернет, что подвергло риску данные о примерно 157 000 клиентах, включая их имена, адреса и банковские реквизиты.

В тот же день несколько сотрудников TalkTalk получили электронные сообщения с требованием выкупа в биткойнах. В качестве доказательства получения доступа к базе данных, преступники описали ее структуру.

Благодаря тому, что компания TalkTalk сообщила о взломе, в октябре и ноябре 2015 г. полиция, при поддержке специалистов из Национального агентства по борьбе с преступностью, арестовала основных подозреваемых (все находились в Великобритании).

Эта атака показала, что даже крупным организациям с высоким уровнем осведомленности об угрозах не удается полностью избавиться от уязвимостей. Их использование может иметь непропорционально серьезный эффект в контексте ущерба для репутации и срыва деятельности, и это происшествие привлекло больше внимание СМИ. Благодаря тому, что компания TalkTalk оперативно сообщила о взломе, правоохранительные органы смогли своевременно среагировать, а общественность и правительство — принять меры для смягчения последствий возможной утечки конфиденциальных данных. В результате этого инцидента компания TalkTalk потеряла примерно 60 млн фунтов и 95 000 клиентов, а стоимость ее акций резко упала.

ПРИМЕР ИЗ ПРАКТИКИ 2: АТАКА НА СИСТЕМУ SWIFT БАНКА БАНГЛАДЕШ

Общество всемирных межбанковских финансовых каналов связи (SWIFT) — международная банковская система,

позволяющая финансовым организациям безопасным способом отправлять и получать информацию о финансовых транзакциях. Поскольку SWIFT отправляет платежные поручения, по которым производятся расчеты между корреспондентскими счетами, обслуживающими соответствующие банки, всегда существовала обеспокоенность по поводу того, что безопасность этого процесса подвергается риску нарушения со стороны киберпреступников или иных злоумышленников, которые могут пропустить через эту систему незаконные платежные поручения или, в худшем случае, остановить или нарушить работу самой сети SWIFT.

В начале февраля 2016 г. некий злоумышленник получил доступ к платежной системе SWIFT Банка Бангладеш и оправил поручения Федеральному Резервному банку Нью-Йорка перевести деньги со счета Банка Бангладеш на банковские счета на Филиппинах. Общая сумма покушения на мошенничество составила 951 млн долларов США. Попытка осуществления 30 транзакций на сумму 850 млн долл. США была предотвращена банковской системой. Однако пять транзакций на сумму 101 млн долл. США были осуществлены. 20 млн долл. США, отслеженные в Шри-Ланке, были возвращены. Оставшийся 81 млн долл. США, переведенный на Филиппины, был отмыт через казино, и часть этих денег была затем отправлена в Гонконг.

Криминалистическая экспертиза, инициированная Банком Бангладеш, обнаружила в банковских системах вредоносное программное обеспечение для сбора данных о процедурах, используемых банком при обработке международных платежей и переводе средств. В ходе дальнейшего анализа программного обеспечения, связанного с осуществлением атаки, которое выполнили специалисты компании BAE Systems, были обнаружены изощренные функциональные средства, поддерживающие взаимодействие с программным обеспечением SWIFT Alliance Access, используемым в инфраструктуре Банка Бангладеш. Специалисты BAE пришли к выводу, «что преступники осуществляют все более изощренные атаки против своих жертв среди организаций, особенно в области проникновения в сеть».

ПРИМЕР ИЗ ПРАКТИКИ 3: АТАКА НА ЭЛЕКТРИЧЕСКУЮ СЕТЬ УКРАИНЫ

В результате кибератаки на украинские электрораспределительные предприятия «Прикарпатьеоблэнерго» и «Киевоблэнерго», имевшей место 23 декабря 2015 г., произошло масштабное отключение энергии и была нарушена работа более 50 подстанций в распределительных сетях. Перерыв электроснабжения в регионе длился в течение нескольких часов, при этом многие другие люди и территории испытали менее значительные перерывы в электроснабжении, а без электричества осталось более 220 000 жителей.

Некоторые пришли к выводу, что атака была осуществлена с использованием вредоносной программы BlackEnergy3, после того как в сети были выявлены образцы программы. Как минимум за шесть месяцев до атаки преступники разослали фишинговые сообщения персоналу энергокомпаний в Украине, содержащие документы Microsoft Office с вредоносным кодом. Однако вряд ли сама программа отключила автоматические выключатели, что привело к прерыванию энергоснабжения. Вероятно, вредоносная программа позволила преступникам собрать учетные данные, с помощью которых они получили удаленный доступ непосредственно к тем аспектам сети, которые впоследствии и дали им возможность отключить электроснабжение.

Это украинское происшествие является первым в мире подтвержденным случаем вывода из строя электрической сети в результате кибератаки. Подобные случаи еще раз демонстрируют необходимость внедрения надежных практических мер безопасности в

масштабах всей критической национальной инфраструктуры (КНИ) для предотвращения подобных инцидентов в Великобритании.

УЯЗВИМОСТИ

Растущее разнообразие устройств

3.15. Когда в 2011 году была опубликована Национальная Стратегия кибербезопасности, большинство людей воспринимало кибербезопасность через призму защиты устройств, таких как компьютеры или ноутбуки. С тех пор активизировалась интеграция интернета во все сферы нашей жизни, и во многом мы этого не осознаем. «Интернет вещей» открывает новые возможности для злоумышленников и повышает вероятность атак, способных причинить физический ущерб, травмы и, в худшем случае, смерть.

3.16. Быстрое внедрение возможностей подключения в критически важных промышленных системах управления процессами в целом ряде таких отраслей, как энергетика, добыча полезных ископаемых, сельское хозяйство и авиация, привело к возникновению «промышленного интернета вещей». Это открывает возможности для взлома устройств и процессов, которые в прошлом были неуязвимы для такого вмешательства, что может иметь катастрофические последствия.

3.17. Таким образом, нам грозят опасности, связанные не только с ненадлежащей кибербезопасностью наших собственных устройств, но и с взаимосвязанностью систем, имеющей фундаментальное значение для нашего общества, здоровья и благосостояния.

Низкий уровень элементарных правил кибербезопасности и соблюдения нормативных требований

3.18. В Великобритании уровень осознания технических уязвимостей программного обеспечения и сетей, равно как и необходимости использования элементарных правил кибербезопасности, несомненно, повысился за последние пять лет. Это, с одной стороны, является результатом таких инициатив, как правительственный план «10 шагов к кибербезопасности», а с другой — огласки, которую получили кибер-происшествия, имеющие негативные последствия для правительств и корпораций. Кибератаки не всегда бывают изощренными или неизбежными, а часто являются результатом использования уязвимостей, которые можно легко устранить и предотвратить. В большинстве случаев, именно уязвимость жертвы, а не изобретательность преступника, является фактором, определяющим успех кибератаки. Компании и организации принимают решения о вложении средств в кибербезопасность, исходя из оценки эффективности затрат, и в конечном итоге несут ответственность за безопасность своих данных и систем. Снизить вероятность кибератаки можно только за счет достижения необходимого баланса между риском нарушения безопасности критически важных систем и конфиденциальных данных, с одной стороны, и вложением достаточных средств в людей, технологии и управление, с другой стороны.

«Не существует системы информационной безопасности, способной предупредить вероятность того, что хотя бы один человек из ста не откроет фишинговое сообщение, и этого может быть достаточно для злоумышленника».

Киаран Мартин, генеральный директор по кибербезопасности, GCHQ, июнь 2015 г.

Низкий уровень подготовки и квалификаций

3.19. Нам не хватает квалифицированных кадров и знаний, чтобы удовлетворить потребности в кибербезопасности в масштабах всего государственного и частного сектора. В компаниях уровень осведомленности о кибербезопасности среди персонала является низким, и сотрудники не понимают своей ответственности в этом отношении, что

частично объясняется недостаточным уровнем планового обучения. Население также недостаточно осведомлено о кибербезопасности.

«Менее пятой части компаний организовали тренинг по вопросам кибербезопасности для своих сотрудников в прошлом году».

Опрос мнений о нарушениях кибербезопасности, 2016 г.

3.20. Мы также должны готовить специалистов и развивать возможности, которые позволят нам идти в ногу с быстро эволюционирующими технологиями и управлять кибер-рисками. Недостаток квалифицированных кадров представляет собой уязвимость на национальном уровне, которую необходимо устранить.

Устаревшие системы и неисправленные уязвимости

3.21. Многие организации в Великобритании продолжают использовать уязвимые устаревшие системы вплоть до следующего этапа модернизации своих ИТ-систем. В этих системах часто используются более старые, неисправленные версии программного обеспечения. Злоумышленники находят уязвимости в таких устаревших версиях, имея необходимые средства для их использования. Другая проблема заключается в использовании некоторыми организациями неподдерживаемого программного обеспечения, для которого нет режима исправления.

«Нами недавно проанализировано 115 000 устройств Cisco, используемых в интернете и в средах наших клиентов, с целью привлечения внимания к рискам безопасности, связанным с устаревшей инфраструктурой, и обнаружили отсутствие должного внимания к вопросу устранения уязвимостей... Анализ показал, что 106 000 из 115 000 устройств содержат известные уязвимости в используемом ими программном обеспечении».

Ежегодный отчет Cisco по информационной безопасности, 2016 г.

Доступность хакерских ресурсов

3.22. Доступность в интернете хакерской информации и простых в использовании хакерских инструментальных средств дает в распоряжение тех, кто заинтересован в развитии хакерских возможностей, все необходимое. Информация, необходимая хакерам для успешного взлома, часто находится в открытом доступе и получить ее можно достаточно быстро. Каждый человек, от простого обывателя до члена совета директоров, должен осознавать уровень опасности, грозящей его персональным данным и системам в интернете, и степень их уязвимости к злонамеренным кибератакам в этой связи.

«99,9% использованных уязвимостей были использованы злоумышленниками более чем через год после того, как была опубликована информация о них».

Отчет о расследованиях Verizon 2015 Data Breach

ВЫВОДЫ

3.23. Благодаря политике Великобритании и учреждению соответствующих институтов, повысился уровень нашей защиты и были смягчены некоторые риски, стоящие перед нами в киберпространстве.

3.24. Однако нам пока еще не удается опережать эти угрозы. Типы кибер-злоумышленников, с которыми нам приходится иметь дело, и их мотивация, в значительной мере, остаются неизменными, даже на фоне существенного роста объемов вредоносных программ и количества таких злоумышленников. Увеличились возможности наших противников, имеющих в своем арсенале самые совершенные технические средства. Речь идет о некоторых государствах и элитных киберпреступниках. Наша общая задача — обеспечить совершенствование и повышение гибкости средств защиты с тем, чтобы сократить возможности атак со стороны злоумышленников и устранить главные причины возникновения уязвимостей, описанных выше.

4. НАЦИОНАЛЬНОЕ ПРОТИВОДЕЙСТВИЕ

4.1. Для смягчения многочисленных рисков, стоящих перед нами, и защиты наших интересов в киберпространстве нам необходим стратегический подход, который ляжет в основу всех коллективных и индивидуальных действий в цифровом пространстве в течение следующих пяти лет. В настоящем разделе изложены наше видение и стратегический подход.

НАШЕ ВИДЕНИЕ

4.2. Согласно нашему видению, к 2021 году в Великобритании будут обеспечены безопасность, устойчивость к киберугрозам, процветание и условия для уверенного пользования цифровыми технологиями.

4.3. Для претворения этого видения в жизнь мы направим усилия на достижение следующих целей:

• **ОБОРОНА** У нас есть средства для защиты Великобритании от эволюционирующих киберугроз, для эффективного реагирования на происшествия и для обеспечения безопасности и устойчивости британских сетей, данных и систем. Граждане, компании и организации государственного сектора обладают необходимыми знаниями и способны защитить себя.

• **СДЕРЖИВАНИЕ** Великобритания не будет легкой целью для агрессии в киберпространстве в какой бы то ни было форме. Мы способны обнаруживать, понимать, расследовать и срывать попытки враждебных действий, направленных против нас, преследуя и наказывая преступников. У нас есть средства для применения наступательных мер в киберпространстве, если мы сочтем это целесообразным.

• **РАЗВИТИЕ** У нас есть инновационная, развивающаяся индустрия кибербезопасности, опирающаяся на научно-технические достижения и разработки на уровне лучших мировых стандартов. У нас есть самодостаточный кадровый резерв, отвечающий национальным потребностям в масштабах государственного и частного сектора. Наши передовые аналитические технологии и опыт помогут Великобритании преодолеть будущие угрозы и вызовы.

4.4. В стремлении к достижению этих целей мы будем осуществлять **МЕЖДУНАРОДНУЮ ДЕЯТЕЛЬНОСТЬ** и оказывать влияние путем инвестирования в партнерства. Мы будем формировать мировое развитие киберпространства таким образом, чтобы продвигать свои интересы в экономике и безопасности в целом.

ПРИНЦИПЫ

4.5 При осуществлении деятельности по достижению этих целей Правительство будет соблюдать следующие принципы:

- наши действия и политика будут определяться необходимостью как обеспечения защиты людей, так и повышения благосостояния страны;
- мы будем относится к угрозе кибератаки не менее серьезно, чем к угрозе сопоставимой «традиционной» атаки, и будем использовать все необходимое для своей защиты;
- мы будем действовать в соответствии с национальным и международным законодательством, ожидая того же и от других;
- мы будем неукоснительно защищать и продвигать наши главные ценности — демократия, верховенство права, свобода, открытость и подотчетность правительства и его институтов, права человека и свобода слова;
- мы будем сохранять и защищать право британских граждан на неприкосновенность их частной жизни;
- мы будем сотрудничать с нашими партнерами. Только в сотрудничестве с

Правительствами Шотландии, Уэльса и Северной Ирландии, со всеми областями государственного сектора, компаниями, институтами и отдельными гражданами мы сможем успешно защитить Великобританию в киберпространстве;
• Правительство будет выполнять свои обязанности и возглавит деятельность по национальному противостоянию угрозам, при этом компании, организации и отдельные граждане отвечают за принятие разумных мер по своей защите в сети и обеспечению устойчивости и работоспособности своих систем в случае атаки;
• ответственность за безопасность организаций в рамках всего государственного сектора, в том числе за кибербезопасность и защиту сетевых данных и услуг, возлагается на соответствующих министров, постоянных секретарей и дирекции;
• мы не допустим возникновения существенного риска для населения и страны в целом в результате того, что компании и организации не приняли необходимых мер для управления киберугрозами;
• мы будем тесно сотрудничать со странами, которые разделяют наши взгляды и с которыми у нас совпадают цели в контексте безопасности, признавая, что киберугрозы не знают границ. Мы также расширим круг сотрудничества с международными партнерами в целях охвата более широких слоев общества, признавая тем самым значение широкой коалиции;
• для обеспечения результативности мер, предпринимаемых Правительством в контексте национальной кибербезопасности и устойчивости к угрозам, мы планируем осуществлять определение, анализ и представление данных, необходимых для измерения состояния коллективной кибербезопасности и успеха в достижении стратегических целей.

РОЛИ И ОБЯЗАННОСТИ

4.6. Для обеспечения безопасности национального киберпространства требуются коллективные усилия. Каждому из нас в этом процессе отводится важная роль.

Отдельные граждане

4.7. Как граждане, сотрудники и потребители, мы принимаем практические меры для защиты своих ценных активов в физическом мире. В виртуальном мире мы должны делать то же самое. Это означает исполнение наших персональных обязанностей по принятию разумных мер для защиты не только аппаратного обеспечения — 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.

Компании и организации

4.8. Компании и организации частного и государственного сектора, а также другие институты хранят персональные данные, предоставляют услуги и эксплуатируют системы в цифровом пространстве. Возможность подключения к этой информации революционно изменила способ их работы. Но вместе с этой технологической трансформацией наступает ответственность за защиту активов, которые они хранят, обеспечение услуг, которые они предоставляют, и интеграцию соответствующего уровня безопасности в продукты, которые они продают. Граждане, потребители и общество в целом рассчитывают на то, что компании и организации примут все разумные меры для защиты их персональных сведений и обеспечения устойчивости — способности выдерживать атаки и восстанавливаться — систем и структур, от которых они зависят. Компании и организации также должны понимать, что, если они станут жертвой

кибератаки, они несут ответственность за ее последствия.

Правительство

4.9. Главная обязанность Правительства — защита государства от атак извне, защита граждан и экономики от убытков и бед и учреждение отечественных и международных структур для защиты их интересов, гарантии основополагающих прав и привлечения преступников к ответственности.

4.10. Правительство, как держатель большого объема данных и поставщик услуг, принимает строгие меры для защиты своих информационных активов. Еще одной важной обязанностью Правительства является консультирование и информирование граждан и организаций о том, что им необходимо сделать для своей защиты в сети, и, где это необходимо, установление стандартов, соответствия которым мы ожидаем от ключевых компаний и организаций.

4.11. Хотя ключевые сектора экономики находятся в частном секторе, в конечном итоге именно Правительство несет ответственность за обеспечение устойчивости на национальном уровне и, совместно со своими партнерами в органах управления, — за функционирование важных услуг и служб и в масштабах всего правительства.

Движущая сила перемен: роль рынка

4.12. Стратегия 2011 года и Программа национальной безопасности преследовали достижение результатов и расширение потенциала как государственного, так и частного сектора из расчета на то, что рынок будет способствовать формирования правильных моделей поведения. Мы ожидали, что соображения коммерческой необходимости и инициированные правительством стимулы, обеспечат вложение компаниями адекватных средств в обеспечение надлежащей кибербезопасности, будут стимулировать поток инвестиций в отрасль и обеспечат формирование адекватного кадрового резерва для этого сектора.

4.13. Многое было достигнуто. В экономической сфере и в обществе в целом за последние пять лет повысился уровень осведомленности о рисках и осознания важности мер, нацеленных на снижение кибер-рисков. Но сочетания рыночных сил и правительственных стимулов само по себе было недостаточно для защиты наших долгосрочных интересов в киберпространстве требуемыми темпами. Слишком высок процент сетей, в том числе в критически важных секторах, которые еще не защищены должным образом. Рынок недооценивает кибер-риски и, следовательно, не обеспечивает надлежащего управления ими. Нарушения все еще имеют место во многих организациях, даже на самом элементарном уровне. Слишком мало инвесторов готовы брать на себя риски, связанные с поддержкой предпринимателей в этом секторе. Слишком мало выпускников и других специалистов, имеющих нужные квалификации, выходит из нашей системы образования и обучения.

4.14. Роль рынка остается важной, и в долгосрочной перспективе он должен оказать гораздо большее воздействие, чем когда-либо способно оказать Правительство. Однако неотложная необходимость в устранении угроз, стоящих перед Великобританией, и растущий спектр уязвимостей цифровой среды требуют принятия Правительством гораздо более широкого ряда мер в краткосрочной перспективе.

Движущая сила перемен: расширение роли Правительства

4.15. Таким образом, Правительство должно задать темп деятельности по удовлетворению потребностей страны в области национальной кибербезопасности. Только у Правительства есть возможность привлечь информационно-аналитические и другие активы, необходимые для защиты нашей страны от самых изощренных угроз. Только у Правительства есть возможность активизировать

сотрудничество в масштабе частного и государственного секторов и обеспечить обмен информацией между ними. Правительство, в консультации с отраслевыми специалистами, призвано сыграть ведущую роль в определении эффективных мер кибербезопасности и обеспечить их внедрение.

4.16. Правительство должно существенно повысить уровень национальной кибербезопасности в течение следующих пяти лет. Эта масштабная и качественно новая программа будет сосредоточена на работе в следующих четырех широких областях:

• **Рычаги и стимулы**. Правительство вложит средства в максимальное увеличение потенциала поистине инновационного сектора кибербезопасности в Великобритании. Мы достигнем этого за счет оказания поддержки стартапам и инвестиций в инновации. Мы также будем стремиться к выявлению в системе образования перспективных студентов на ранних стадиях обучения и создавать условия для развития их таланта с тем, чтобы сформировать четкие каналы карьерного роста в этой профессии, которая требует более четкого определения. Правительство также будет использовать все имеющиеся в его распоряжении рычаги, в том числе готовящийся Регламент общей защиты данных (GDPR), для повышения стандартов кибербезопасности в масштабах национальной экономики, включая, если это необходимо, регулятивные меры.

• **Расширение деятельности разведывательных и правоохранительных органов в области кибербезопасности.** Разведывательные органы, министерство обороны, полиция и Национальное агентство по борьбе с преступностью, координируя усилия с международными партнерскими агентствами, должны расширить усилия по определению, предупреждению и пресечению враждебной деятельности со стороны иностранных субъектов, киберпреступников и террористов. Это поможет усовершенствовать сбор и использование разведывательной информации в целях получения упреждающих разведданных о намерениях и возможностях наших противников.

• **Разработка и развертывание технологий**, в том числе мер Активной киберзащиты, в партнерстве с отраслевыми предприятиями, в целях углубления нашего понимания угроз, укрепления безопасности британских систем и сетей государственного и частного сектора, перед лицом этих угроз, а также пресечения вредоносной деятельности.

• **Национальный центр кибербезопасности (NCSC)**. Правительство учредило единый центральный орган по кибербезопасности на национальном уровне. Эта организация будет управлять кибер-происшествиями и призвана стать авторитетным центром передового опыта в области кибербезопасности, а также предоставлять индивидуальную поддержку и рекомендации департаментам, правительствам Шотландии, Уэльса и Северной Ирландии, регулирующим органам и компаниям. NCSC будет заниматься анализом, обнаружением и изучением киберугроз, а также давать консультации по кибербезопасности в поддержку деятельности Правительства, направленной на активизацию инноваций, содействие успешному развитию отрасли кибербезопасности и созданию кадрового резерва в этой области. Уникальным отличием этого взаимодействующего с общественностью органа, является то, что его головным учреждением будет GCHQ. Поэтому он сможет опираться на первоклассный опыт, знания и возможности, которые имеет эта организация, что позволит ему улучшить деятельность по поддержке экономики и общества в целом. За эффективную реализацию этих рекомендаций по кибербезопасности и далее будут отвечать правительственные департаменты.

«Принимая во внимание промышленные масштабы хищения интеллектуальной собственности из компаний и университетов, а также огромное количество фишинговых сообщений и мошеннических афер с использованием вредоносных программ,

борьба с которыми отнимает много времени и денег, учреждение Национального центра кибербезопасности продемонстрирует, что Великобритания сосредоточивает усилия на противодействии угрозам, существующим в сети».
Роберт Ханнаган, Директор, GCHQ, март 2016 г.

4.17. Для реализации этих изменений в области кибербезопасности и устойчивости потребуются дополнительные ресурсы. В Обзоре стратегической обороны и безопасности за 2015 г., Правительство предусмотрело выделение 1,9 млрд фунтов в течение пяти лет действия данной стратегии на меры по выполнению обязательств и достижению целей, предусмотренных ею.

НАЦИОНАЛЬНЫЙ ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

Национальный центр кибербезопасности (NCSC) был учрежден 1 октября 2016 г. NCSC предлагает уникальную возможность построения эффективных партнерских отношений в области кибербезопасности между правительством, отраслью и обществом для повышения уровня безопасности Великобритании в сети. Он станет центром реагирования на происшествия и авторитетным британским органом в области кибербезопасности. Ключевые сектора впервые получили возможность контактировать непосредственно с персоналом NCSC для получения рекомендаций и поддержки деятельности по защите сетей и систем от киберугроз.

NCSC будет служить:

- единым правительственным источником рекомендаций, касающихся разведданных об угрозах в киберпространстве и информационной безопасности;

- авторитетной, взаимодействующей с общественностью правительственной организацией по противодействию киберугрозам, которая, в тесном сотрудничестве с представителями отрасли, научными кругами и международными партнерам, обеспечивает защиту Великобритании от кибератак;

- взаимодействующей с общественностью организацией, имеющей возможность обращаться к необходимой секретной разведывательной информации и первоклассным техническим возможностям GCHQ.

Будет принят поэтапный подход развития потенциала NCSC в продолжение действия настоящей стратегии. Он объединит возможности, уже наработанные CESG (подразделение GCHQ по информационной безопасности), Центром защиты национальной инфраструктуры (CPNI), Группой быстрого реагирования на чрезвычайные происшествия в области компьютерной безопасности (CERT-UK) и Центром оценки киберугроз (CCA), позволяя нам обращаться к передовым достижениям в этой области, одновременно существенно упростив действующий прежде порядок доступа. Изначально мы сосредоточим усилия на следующем:

- развитие первоклассных возможностей реагирования на кибер-происшествия, позволяющих смягчать их последствия, начиная с инцидентов в отдельных организациях и заканчивая масштабными атаками на национальном уровне;
- предоставление информации о том, как организации частного и государственного сектора могут решать проблемы кибербезопасности, содействуя обмену информацией о киберугрозах;
- дальнейшее предоставление экспертных отраслевых консультаций Правительству и представителям критически важных индустрий, таких как телекоммуникационная, энергетическая и финансовая, а также предоставление

рекомендаций по кибербезопасности в масштабах всей Великобритании.

Через NCSC Правительство сможет эффективно реализовать целый ряд элементов настоящей стратегии. Мы понимаем, что по мере развития NCSC, возникнет необходимость переориентации его фокуса и возможностей в зависимости от новых вызовов и накопленного опыта.

ПЛАН РЕАЛИЗАЦИИ

Наши цели в области кибербезопасности государства в течение следующих пяти лет обоснованно масштабны. Чтобы их достичь, мы должны действовать последовательно и решительно в масштабах всего цифрового пространства. Деятельность по воплощению видения Правительства в жизнь ориентирована на достижение трех основных целей стратегии — ОБОРОНА киберпространства, СДЕРЖИВАНИЕ противников и РАЗВИТИЕ потенциала — и опирается на эффективную МЕЖДУНАРОДНУЮ ДЕЯТЕЛЬНОСТЬ.

5. ОБОРОНА

5.0.1. ОБОРОННАЯ составляющая настоящей стратегии нацелена на обеспечение устойчивости британских сетей, данных и систем, используемых в государственной, коммерческой и частной сферах, и их защиты от кибератак. Невозможно предотвратить каждую кибератаку, так же как невозможно предупредить каждое преступление. Однако Великобритания, вместе с ее гражданами, образовательными организациями, научным сообществом, деловыми кругами и другими правительствами, может построить многоуровневую систему защиты, которая существенно сократит риск возникновения кибер-происшествий, защитит самые ценные активы и позволит нам всем успешно и прибыльно пользоваться киберпространством. Действия, нацеленные на укрепление сотрудничества между государствами и внедрение передовых методов кибербезопасности, также в интересах нашей коллективной безопасности.

5.0.2. Правительство примет меры для обеспечения доступа граждан, компаний, организаций и институтов государственного и частного сектора к информации о том, как правильно защитить себя. Национальный центр кибербезопасности будет служить единым государственным источником правительственных рекомендаций по вопросам аналитики угроз и информационной безопасности, обеспечивая нам доступ к индивидуализированным руководствам по кибероборонe и помогая оперативно и эффективно реагировать на крупные происшествия в киберпространстве. Правительство, совместно с отраслевыми и международными партнерами, определит, какой должна быть эффективная кибербезопасность для предприятий государственного и частного сектора, для наших самых важных систем и служб и для экономики в целом. Мы обеспечим безопасность по умолчанию во всех новых правительственных и критически важных системах. Правоохранительные органы будут тесно сотрудничать с отраслью и Национальным центром кибербезопасности над предоставлением динамической разведывательной информации о криминальных угрозах, которая позволит предприятиям надежнее защитить себя, и над продвижением стандартов и рекомендаций по безопасности.

5.1. АКТИВНАЯ КИБЕРЗАЩИТА

5.1.1. Активная киберзащита (АКЗ) — принцип реализации мер безопасности для укрепления защиты сетей или систем с целью повышения их устойчивости к атакам. В коммерческом контексте Активная киберзащита, как правило, относится к наработке аналитиками понимания угроз для безопасности их сетей с последующей разработкой и внедрением мер по инициативному противодействию этим угрозам и защите от них. В контексте настоящей стратегии Правительство применяет этот же принцип в более широком масштабе: Правительство будет использовать все имеющиеся в его распоряжении уникальные знания, опыт, возможности и влияние для достижения качественных изменений национальной кибербезопасности с целью эффективного реагирования на киберугрозы. «Сеть», которую мы стремимся защитить, — это все британское киберпространство. Предложенные

мероприятия представляют собой план оборонных действий, опирающийся на опыт и знания NCSC, выступающего в качестве Национального технического эксперта в деятельности по реагированию на киберугрозы в Великобритании на макроуровне.

Цели

5.1.2. При осуществлении АКЗ Правительство преследует
следующие цели:

- превращение Великобритании в гораздо более трудно поражаемую цель для субъектов, спонсируемых государствами, и киберпреступников путем повышения устойчивости британских сетей;
- отражение основного объема массовых/не особенно изощренных вредоносных атак на британские сети путем блокирования вредоносных коммуникаций между хакерами и их жертвами;
- совершенствование и увеличение объема и масштаба возможностей Правительства по противодействию серьезным угрозам со стороны злоумышленников, спонсируемых государствами, и киберпреступников;
- обеспечение защиты интернет- и телекоммуникационного трафика от взлома злоумышленниками;
- укрепление защиты британской критической инфраструктуры и услуг, ориентированных на граждан, от киберугроз;
- разрушение бизнес-модели злоумышленников любого вида, лишение их мотивации и сокращение урона, который могут причинить их атаки.

Подход

5.1.3. В ходе реализации этих целей Правительство будет:

- сотрудничать с представителями отрасли, прежде всего с операторами связи, над тем, чтобы затруднить атаки на британские интернет-службы и пользователей и значительно сократить вероятность длительных последствий в случае атаки на Великобританию. Сюда входит борьба с фишингом, блокировка вредоносных доменов и IP-адресов и другие мероприятия по пресечению атак с использованием вредоносного программного обеспечения. Сюда также войдут меры по обеспечению безопасности британской инфраструктуры маршрутизации телекоммуникационного и интернет-трафика;
- содействовать расширению и развитию возможностей GCHQ, министерства обороны и Национального агентства по борьбе с преступностью в области пресечения серьезных киберугроз для Великобритании, в том числе изощренных кампаний со стороны киберпреступников и враждебных иностранных субъектов;
- совершенствовать защиту правительственных систем и сетей, поддерживать усилия отрасли по повышению уровня встроенной безопасности цепочек поставки CNI, повышать безопасность экосистемы программного обеспечения в Великобритании и обеспечивать автоматическую защиту государственных интернет-услуг для граждан.

5.1.4. Эти инициативы, по возможности, будут реализованы совместно с нашими партнерами в отрасли или через партнерство с ними. Представители отрасли будут заниматься разработкой и руководством основного объема деятельности по внедрению, тогда как вклад Правительства будет заключаться в предоставлении экспертной поддержки, рекомендаций и идейного руководства.

5.1.5. Правительство также предпримет конкретные действия по реализации этих мер, в том числе:

• блокирование вредоносных атак совместно с операторами связи. Для достижения этого мы ограничим доступ к определенным доменам или веб-сайтам, являющимся известными источниками вредоносного программного обеспечения. Это называется блокированием/фильтрацией через систему доменных имен (DNS);
• предупреждение фишинговой деятельности, осуществляемой с помощью «спуфинга» доменов (когда мошенническое электронное сообщение выглядит так, будто оно отправлено банком или правительственным органом) путем развертывания в правительственных сетях системы верификации электронных сообщений в качестве стандартной защитной меры и поощрения предприятий отрасли последовать этому примеру;
• продвижение передовых методик обеспечения безопасности с помощью организаций по управлению использованием интернета, в которых участвуют многие заинтересованные стороны, таких как Корпорация по управлению доменными именами и IP-адресами (ICANN), которая занимается регулированием вопросов, связанных с доменными именами, Инженерный совет интернета (IETF) и Европейские региональные интернет-регистраторы (RIPE), и путем вовлечения заинтересованных сторон в работу Форума ООН по управлению интернетом (IGF);
• сотрудничество с правоохранительными органами в целях защиты британских граждан от кибератак со стороны незащищенной зарубежной инфраструктуры;
• работа по внедрению средств контроля в целях защиты маршрутизации интернет-трафика правительственных органов и предотвращения попыток его незаконной перемаршрутизации со стороны злонамеренных субъектов;
• вложение средств в программы министерства обороны, NCA и GCHQ, призванные расширить возможности этих организаций по реагированию на серьезные атаки на британские сети со стороны злоумышленников, спонсируемых государствами, и киберпреступников, и их пресечению.

Мы будем разрабатывать такие технические мероприятия по мере эволюции угроз, чтобы обеспечить автоматическую защиту британских граждан и бизнеса от основного числа масштабных кибератак, осуществляемых с использованием массового вредоносного программного обеспечения.

Измерение успеха

5.1.6. Правительство будет измерять успех своей деятельности по внедрению эффективных средств АКЗ путем оценки прогресса в достижении следующих результатов:

• в Великобритании стало сложнее осуществлять фишинговую деятельность, так как мы обеспечили масштабную защиту от использования вредоносных доменов, внедрили более активную и масштабную защиту от фишинга, равно как и других форм коммуникаций в рамках атак социальной инженерии, например, «вишинга» и SMS-спуфинга;
• блокируется гораздо более значительная часть вредоносных коммуникаций и технических артефактов, связанных с кибератаками и использованием уязвимостей;
• британский интернет- и телекоммуникационный трафик стал значительно менее уязвим к попыткам перемаршрутизации со стороны злонамеренных субъектов;
• существенно расширились возможности GCHQ, вооруженных сил и NCA по реагированию на серьезные

угрозы со стороны субъектов, спонсируемых государствами, и преступников.

5.2. ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ИНТЕРНЕТА

5.2.1. С развитием технологий у нас появляется возможность существенно ослабить способность наших противников к осуществлению киберпреступной деятельности в Великобритании, за счет того, что поставляемые в будущем продукты и услуги, имеющие выход в сеть, будут «безопасными по умолчанию». Это означает, что настройки безопасности, встроенные в используемое нами программное и аппаратное обеспечение, активируются производителем по умолчанию, обеспечивая для пользователей максимальный уровень безопасности, и для их изменения пользователи должны будут предпринять определенные действия. Сложность заключается в том, чтобы совершить этот трансформационный переворот таким способом, чтобы обеспечить поддержку конечного пользователя и поставку коммерчески жизнеспособных продуктов или услуг и вместе с тем сохранить свободную и открытую природу интернета.

«Количество подключенных к сети устройств стремительно увеличивается. Мы наблюдали большое количество демонстрационных и реальных атак в 2015 году, способствовавших обнаружению серьезных уязвимостей в автомобилях, медицинских устройствах и других продуктах. Производители должны сделать безопасность приоритетной задачей, чтобы сократить риск серьезных последствий для личности, экономики и общества».
Отчет Symantec об угрозах безопасности, 2016 г.

5.2.2. Правительство имеет все необходимое для того, чтобы возглавить деятельность по изучению новых технологий, способных эффективнее защитить наши системы, помочь предприятиям отрасли повысить уровень безопасности цепей поставки, защитить экосистему программного обеспечения и обеспечить автоматическую защиту граждан, получающих доступ к государственным услугам через интернет. Правительство должно испытать и внедрить новые технологии, обеспечивающие автоматическую защиту государственных продуктов и услуг, предоставляемых через интернет. Подобные технологии по возможности должны быть доступны для организаций частного сектора и отдельных граждан.

Цель

5.2.3. Основной объем продуктов и услуг в сетевом доступе будет «защищен по умолчанию» к 2021 г. У потребителей будет право выбирать продукты и услуги, в которых встроенная защита является настройкой по умолчанию. Пользователи смогут отключать эти настройки, если захотят, тогда как потребители, желающие взаимодействовать с киберпространством самым безопасным способом, будут защищены автоматически.

Наш подход

5.2.4. Мы будем осуществлять следующие действия:

- Правительство будет подавать пример, предоставляя защищенные интернет-услуги, безопасность которых не зависит от безопасности самого интернета;
- Правительство будет изучать возможности для сотрудничества с представителями отрасли, с перспективой разработки передовых способов повышения безопасности аппаратного и программного обеспечения «по умолчанию»;
- мы внедрим сложные новые технологии кибербезопасности в правительственные системы, поощряя правительства Шотландии, Уэльса и Северной Ирландии последовать нашему примеру, с тем, чтобы сократить предполагаемые риски в связи с таким внедрением. Это позволит доказать эффективность и продемонстрировать

преимущества новых технологий и подходов с точки зрения безопасности. Это также поставит безопасность в основу разработки новых продуктов, ликвидируя возможности для их использования в преступных целях и, следовательно, защищая конечного пользователя.

5.2.5. В этих целях мы будем:

• и далее поощрять поставщиков аппаратного и программного обеспечения продавать продукты, в которых настройки безопасности установлены по умолчанию, что требует активных действий со стороны пользователя для их деактивации и, как следствие, снижения уровня безопасности. Некоторые поставщики уже делают это, хотя еще не все принимают эти необходимые меры;
• и далее развивать службы оценки репутации IP-адресов в целях защиты государственных цифровых услуг (это позволит поставщиком интернет-услуг получать информацию об IP-адресах, с которых осуществляется подключение к ним, помогая принимать более информированные решения по управлению рисками в режиме реального времени);
• стремиться устанавливать в правительственных сетях продукты, дающие уверенность в правильной работе программного обеспечения и отсутствии злонамеренного вмешательство в его работу;
• изучать возможности внедрения механизмов, уведомляющих пользователей о том, что они используют устаревшие браузеры, и за пределами домена GOV.UK — в других системах оказания цифровых услуг;
• вкладывать средства в такие технологии, как спецификация Trusted Platform Modules (TPM) и новые отраслевые стандарты, такие как Fast Identity Online (FIDO), поддерживающие аутентификацию пользователей без необходимости ручного ввода пароля, а с использованием машин и иных устройств, имеющихся в распоряжении пользователя. Правительство осуществит тестирование инновационных механизмов аутентификации, чтобы продемонстрировать их возможности в контексте безопасности и удобства пользования в целом.

5.2.6. Правительство также будет изучать возможности для стимулирования рынка путем использования рейтингов безопасности для новых продуктов, чтобы у потребителей была четкая информация о том, какие продукты и услуги обеспечивают для них самый высокий уровень безопасности. Правительство также изучит возможности увязывания таких рейтингов безопасности продуктов с новыми и существующими регламентами, и изучит возможные способы предупреждения потребителей о том, что действия, которые они собираются совершить в сети, грозят нарушению их безопасности.

Измерение успеха

5.2.7. Правительство будет измерять успех своей деятельности по повышению безопасности интернета путем оценки прогресса в достижении следующих результатов:

• большая часть продуктов потребления и услуг, доступных в Великобритании в 2021 г., способствует максимальному повышению безопасности Великобритании, благодаря автоматической активации в них встроенных настроек «безопасности по умолчанию» или обеспечению безопасности на этапе проектирования;
• население Великобритании уверенно пользуется всеми государственными услугами, предоставляемыми на уровне национальных и местных органов, а также правительств Шотландии, Уэльса и

Северной Ирландии, поскольку они максимально защищены, а уровни вероятного мошенничества находятся в пределах приемлемых параметров риска.

5.3. ЗАЩИТА ПРАВИТЕЛЬСТВА

5.3.1. Правительства Великобритании, Шотландии, Уэльса и Северной Ирландии и государственный сектор в целом сохраняют большое количество конфиденциальных данных. Они предоставляют важные услуги населению и эксплуатируют сети, имеющие критическое значение в контексте национальной безопасности и устойчивости к угрозам. Правительственные системы лежат в основе функционирования нашего общества. Модернизация сектора государственных услуг и далее будет краеугольным камнем Британской стратегии по развитию цифровых технологий с целью вывода Великобритании на передовые мировые позиции в цифровом пространстве.
Чтобы сохранить доверие граждан к сетевым услугам и системам государственного сектора, правительство должно обеспечить защиту имеющихся в его распоряжении данных, а органы всех ветвей власти должны внедрить соответствующие уровни кибербезопасности перед лицом постоянных атак со стороны злоумышленников, нацеленных на получение доступа к сетям и данным правительства и государственного сектора.

Цели

5.3.2. Мы стремимся к достижению следующих результатов:

- граждане уверенно пользуются электронными услугами, предоставляемыми правительством: они уверены в безопасности своей конфиденциальной информации и, в свою очередь, осознают свою ответственность за безопасный способ подачи своей конфиденциальной информации;
- Правительство установит и будет соблюдать соответствующие стандарты кибербезопасности, обеспечивая понимание и соблюдение всеми государственными органами своих обязательств по защите сетей, данных и услуг;
- критически важные активы Правительства, в том числе чрезвычайно секретные, защищены от кибератак.

Наш подход

5.3.3. Британское Правительство продолжит расширять ряд услуг, предоставляемых через интернет, с тем, чтобы Великобритания стала настоящим «цифровым по умолчанию» государством. Государственная цифровая служба (GDS), Государственная коммерческая служба (CCS) и NCSC должны обеспечивать, чтобы все новые цифровые услуги, предлагаемые или получаемые правительством, также были «безопасными по умолчанию».

5.3.4. Государственные сети имеют весьма сложную структуру, и многие из них все еще используют устаревшие системы, а также коммерческое программное обеспечение, которое уже не обслуживается поставщиком. Мы обеспечим отсутствие каких-либо неуправляемых рисков в связи с использованием устаревших систем и неподдерживаемого программного обеспечения.

5.3.5. Мы повысим устойчивость правительства и государственного сектора в целом к кибератакам. В этой связи мы должны обеспечить наличие точных и актуальных сведений обо всех системах, данных и пользователях, имеющих к ним доступ. Вероятность и воздействие кибер-происшествия будут сведены к минимуму за счет внедрения передовых методик в соответствии с рекомендациями NCSC. Правительство также обеспечит возможность эффективного реагирования на кибер-происшествия путем внедрения программы

отработки действий в случае происшествий и регулярного тестирования правительственных сетей. Мы будем привлекать к участию в этой программе Правительства Шотландии, Уэльса и Северной Ирландии и органы местной власти, если это будет целесообразно. Использование механизмов автоматического сканирования поможет нам лучше понимать состояние сетевой безопасности правительства.

5.3.6. Кибербезопасность касается не только технологий. Успеху практически всех состоявшихся кибератак способствовал человеческий фактор. Поэтому мы продолжим вкладывать средства в кадры, чтобы обеспечить понимание кибер-рисков каждым сотрудником государственных органов. Мы наработаем специальные знания в тех областях, где риски являются более высокими, с тем чтобы обеспечить внедрение процессов, необходимых для эффективного управления этими рисками.

5.3.7. NCSC разработает ведущее в мире руководство по кибербезопасности, которое будет обновляться по мере появления новых угроз и разработки новых технологий. Мы постараемся обеспечить для государственных организаций простой доступ к информации об угрозах с тем, чтобы они лучше понимали кибер-риски, стоящие перед ними, и предпринимали необходимые меры.

5.3.8. Мы продолжим работать над усовершенствованием сетей с высоким грифом секретности, чтобы обеспечить надежную защиту наиболее секретных коммуникаций Правительства.

5.3.9. Уникальные вызовы в контексте кибербезопасности связаны с системами здравоохранения и социальной защиты. В этом секторе работает примерно 1,6 млн человек и насчитывается более 40 000 организаций, в которых существует широкое разнообразие ресурсов и возможностей информационной безопасности. Регулятор National Data Guardian for Health and Care установил новые стандарты данных для систем здравоохранения и социальной защиты в Англии, а также новые модели получения согласия на использование данных/отказа от предоставления данных для пациентов. Правительство, совместно с организациями здравоохранения и социальной защиты, будет внедрять эти стандарты.

«Великобритания — один из мировых лидеров о области кибербезопасности, а новый Центр управления кибербезопасностью обеспечит защиту операций наших Вооруженных сил перед лицом растущих угроз. Благодаря увеличению оборонного бюджета мы получаем возможность опережать наших противников в киберпространстве, а также вкладывать средства в развитие обычных боевых возможностей».

Достопочтенный Майкл Фэлон, член парламента,
Министр обороны, апрель 2016 г.

5.3.10. Кибербезопасность имеет жизненно важное значение для обороны нашей страны. При проведении операций как в Великобритании, так за ее пределами Вооруженные силы полагаются на информационные и коммуникационные системы. Инфраструктура и персонал министерства обороны (МО) представляют собой заметные объекты для нападения. Оборонные системы регулярно подвергаются атакам со стороны преступников, иностранных разведслужб и других злоумышленников, стремящихся использовать уязвимости персонала, сорвать их работу и операции, повредить данные и похитить информацию. Чтобы повысить уровень осведомленности об угрозах и улучшить функции обнаружения и реагирования, мы учредим Центр управления кибербезопасностью (CSOC), который будет использовать самые передовые средства кибербезопасности для защиты киберпространства МО и реагирования на угрозы. CSOC, в тесном сотрудничестве с NCSC, будет противостоять вызовам кибербезопасности, стоящим перед МО, и

вносить свой в вклад в обеспечение национальной безопасности в целом.

Измерение успеха

5.3.11. Правительство будет измерять успех своей деятельности по защите государственных сетей, систем и данных путем оценки прогресса в достижении следующих результатов:

- Правительство имеет глубокое понимание уровней риска кибербезопасности в масштабах всего правительства и государственного сектора в целом;
- отдельные правительственные учреждения и другие органы обеспечивают защиту пропорционально уровню риска и в соответствии с согласованными минимальными государственными стандартами;
- правительственные департаменты и другие государственные органы устойчивы к угрозам и способны эффективно реагировать на кибер-происшествия, сохраняя функциональность и обеспечивая быстрое восстановление;
- новые технологии и цифровые сервисы, развертываемые правительством будут иметь настройки «кибербезопасности по умолчанию»;
- мы осведомлены обо всех известных уязвимостях правительственных систем и служб, имеющих выход в интернет, и активно их устраняем;
- все поставщики Правительства обеспечивают соответствие необходимым стандартам кибербезопасности.

5.4. ЗАЩИТА КРИТИЧЕСКОЙ НАЦИОНАЛЬНОЙ ИНФРАСТРУКТУРЫ И ДРУГИХ ПРИОРИТЕТНЫХ СЕКТОРОВ

Контекст

5.4.1 Кибербезопасность определенных британских организаций имеет особое значение, так как в случае успеха кибератаки на них последствия для национальной безопасности страны могут быть чрезвычайно серьезными. Они могут сказаться на жизнедеятельности британских граждан, стабильности и прочности британской экономики и на международном авторитете и репутации Великобритании. В элитную группу этих компаний и организаций государственного и частного сектора, входят предприятия критической национальной инфраструктуры (КНИ), предоставляющие важные услуги государству. Обеспечение безопасности и устойчивости КНИ будет приоритетом деятельности Правительства. В эту элитную группу также входят компании и организации вне КНИ, требующие более высокого уровня поддержки. Среди них:

- бриллианты в нашей экономической короне – самые успешные британские компании и компании, чьи исследования и интеллектуальная собственность гарантируют нашу будущую экономическую мощь;
- держатели данных — причем не только организации, имеющие большие объемы персональных данных, но и организации, хранящие данные об уязвимых гражданах в Великобритании и за рубежом, такие как благотворительные организации;
- первоочередные объекты нападения — такие как СМИ, в случае атаки на которые может пострадать репутация Великобритании и свобода слова или Правительство может лишиться доверия граждан;
- основа нашей цифровой экономики — поставщики цифровых услуг, поддерживающие электронную коммерцию и цифровую экономику, работа которых зависит от доверия потребителей к предоставляемым ими услугам;
- организации, которые, опираясь на рыночные силы и авторитет, могут

оказать влияние на экономику в целом в целях повышения уровня ее кибербезопасности, такие как страховые фирмы, инвестиционные компании, регулирующие органы и профессиональные консультанты.

5.4.2. Необходимо сделать еще многое для защиты этих критически важных составляющих нашей экономики и поддержки организаций, способных оказать сильное влияние на других. Наша КНИ — в контексте как частного, так и государственного сектора — продолжает оставаться объектом для атаки. В масштабе этих и многих других приоритетных секторов кибер-риски все еще недостаточно изучены и не контролируются должным образом, даже на фоне продолжающегося роста и расширения спектра угроз.

«Кибербезопасность имеет ключевое значение для раскрытия инновационного потенциала и развития. Применяя адаптированный к потребностям организации и ориентированный на риски подход к кибербезопасности, организации могут сместить фокус на возможности и исследования. Для компании, успешно работающей в пределах «интернета вещей» и обеспечивающей полную поддержку и защиту людей и их личных мобильных устройств (от простого телефона до медицинского устройства, от небольших интеллектуальных приборов до «умных» автомобилей) укрепление доверия потребителей является ключевым фактором конкурентоспособности и должно стать приоритетным направлением деятельности».

Глобальная информационная безопасность, Опрос EY, 2015 г.

Цель

5.4.3. Правительство Великобритании, в сотрудничестве с Правительствами Шотландии, Уэльса и Северной Ирландии и другими компетентными органами, где это необходимо, обеспечит, чтобы самые важные организации и компании, включая КНИ, имели надлежащий уровень безопасности и устойчивости перед лицом кибератак. Ни Правительство, ни другие государственные органы не возьмут на себя ответственность за управление этими рисками от имени частного сектора, которая справедливо возлагается на советы директоров, владельцев и операторов. Однако Правительство будет оказывать им помощь и поддержку на уровне, соответствующим угрозам, которые стоят перед этими компаниями, и последствиям, которые могут возникнуть в случае атаки на них.

Наш подход

5.4.4. Руководители и советы директоров компаний и организаций несут ответственность за безопасность своих сетей. Они обязаны выявлять критически важные системы и регулярно оценивать их уязвимости с учетом эволюционирующего технологического ландшафта и угроз. Они должны вкладывать средства в технологии и персонал с тем, чтобы избавиться от уязвимостей в текущих и будущих системах и цепочках поставки, а также поддерживать уровень кибербезопасности, пропорциональный риску. Они также должны иметь в своем распоряжении возможности тестирования, чтобы гарантировать способность к реагированию в случае атаки. В том, что касается организаций КНИ, они должны осуществлять это совместно с государственными органами и регулирующими организациями, чтобы у нас была уверенность в том, что кибер-риски управляются надлежащим образом и, если это не так, применять соответствующие меры в интересах национальной безопасности.

5.4.5. Поэтому Правительство должно понимать, каким является уровень кибербезопасности в масштабах всей КНИ, и разработать необходимые меры вмешательства в случае необходимости, чтобы обеспечить улучшение ситуации в национальных интересах.

5.4.6. Правительство будет:

- обмениваться информацией об угрозах, доступной только ему, с представителями предприятий с тем, чтобы они знали, от каких угроз нужно защищаться;
- предоставлять рекомендации и руководства по управлению кибер-рисками и, работая совместно с представителями отрасли и научных кругов, определять эффективные меры кибербезопасности;
- стимулировать внедрение мер повышенной безопасности, необходимой для защиты КНИ, таких как учреждение учебных объектов, испытательных лабораторий, стандартов безопасности и консультационных служб;
- проводить, совместно с компаниями КНИ, учения, призванные помочь им в управлении кибер-рисками и уязвимостями.

5.4.7. NCSC будет предоставлять такие услуги самым важным британским компаниям и организациям, в том числе компаниям КНИ. Осуществлять это он будет в партнерстве с департаментами и регулирующими организациями, которые должны обеспечивать управление кибер-рисками в своих секторах на уровне, необходимом для защиты национальных интересов.

5.4.8. Правительство также позаботится о том, чтобы была разработана и внедрена необходимая структура регулирования кибербезопасности, которая:

- обеспечит принятие представителями отрасли мер для своей защиты от угроз;
- будет ориентированной на достижение результатов и достаточной гибкой для того, чтобы не отставать от угроз, а не просто обеспечивать соблюдение формальностей вместо надлежащего управления рисками;
- будет достаточно адаптивной для того, чтобы способствовать росту и развитию инноваций, а не просто направлять его;
- будет согласованной с регулятивными режимами в других юрисдикциях с тем, чтобы британским компаниям не приходилось иметь дело с фрагментированными и обременительными требованиями;
- в сочетании с эффективной поддержкой Правительства, будет создавать конкурентные преимущества для Великобритании.

5.4.9. Во многих секторах экономики уже действуют регулятивные требования в отношении кибербезопасности. Тем не менее, мы должны обеспечить принятие мер, необходимых для управления рисками для кибербезопасности, в масштабах всей экономики, включая КНИ.

Измерение успеха

5.4.10. Правительство будет измерять успех своей деятельности по защите КНИ и других приоритетных секторов путем оценки прогресса в достижении следующих результатов:

- мы понимаем уровень кибербезопасности в масштабах всей КНИ и предусмотрели необходимые меры вмешательства, чтобы в случае необходимости обеспечить улучшение ситуации в национальных интересах;
- самые важные компании и организации понимают существующий уровень угроз и в соответствии с ним внедряют правила кибербезопасности.

5.5. ИЗМЕНЕНИЕ ПОВЕДЕНИЯ В ОБЩЕСТВЕ И БИЗНЕСЕ

5.5.1 Успех британской цифровой экономики зависит от доверия компаний и населения к интернет-услугам. Британское Правительство, совместно с представителями отрасли и другими составляющими государственного

сектора, работает над повышением уровня осведомленности и понимания угроз. Правительство также предоставляет населению и компаниям доступ к некоторым средствам, необходимым для их защиты. Тогда как существует много организаций, достигших отличных результатов, и зачастую на самом высоком мировом уровне, большинство компаний все еще не имеют управления кибер-рисками на должном уровне в области собственной защиты и предоставления услуг в сети.

«В прошлом году, нарушения, имевшие место в крупных компания, в среднем, обошлись им в 36 500 фунтов. Для небольших фирм эта цифра в среднем составляет 3 100 фунтов. 65% крупных организаций сообщили об имевших место нарушениях информационной безопасности в прошлом году, и в 25% из них нарушения имеют место, по крайней мере, один раз в месяц. Почти семь из десяти атак осуществлялись с использованием вирусов, шпионского или вредоносного ПО, которые могли быть обезврежены, если бы использовалась Правительственная программа Cyber Essentials».

Опрос мнений о проверке состояния и нарушениях кибербезопасности, проведенный Правительством в 2016 г.

Цель

5.5.2. Наша цель — добиться того, чтобы отдельные люди и организации, независимо от размера и отраслевой принадлежности, принимали соответствующие меры для своей защиты и защиты потребителей от урона, который могут причинить кибератаки.

Наш подход

5.5.3. Правительство будет предоставлять рекомендации, необходимые для обеспечения защиты экономики. Мы усовершенствуем способы предоставления таких рекомендаций с целью максимального повышения их эффективности. В том, что касается населения, Правительство будет привлекать авторитетных личностей, чтобы расширить охват наших рекомендаций, а также повысить их значимость и доверие к ним. Мы будем предоставлять рекомендации, легкие для исполнения и актуальные для людей, там, где они получают доступ к услугам и подвергают себя риску. К этой деятельности по необходимости будут привлекаться Правительства Шотландии, Уэльса и Северной Ирландии и другие органы власти.

5.5.4. В том, что касается бизнеса, мы будем работать через организации, такие как страховые компании, регулирующие организации и инвесторы, которые могут оказать влияние на компании с тем, чтобы обеспечить управление кибер-рисками с их стороны. При этом мы будем обращать внимание на очевидные преимущества для бизнеса и оценку стоимости кибер-рисков, сделанную организациями, влияющими на развитие рынка. Мы постараемся лучше понять, почему многие организации все еще не обеспечивают надлежащей защиты, и, совместно с такими организациями, как органы отраслевой стандартизации, сместим акцент с содействия повышению уровня осведомленности на убеждение компаний принять необходимые меры. Мы обеспечим внедрение структуры регулирования, необходимой для управления теми кибер-рисками, которые не были урегулированы рыночными силами. В рамках этой деятельности мы будем стремиться использовать такие рычаги, как GDPR, для утверждения стандартов кибербезопасности и защиты граждан.

5.5.5. Население и организации Великобритании будут иметь доступ к информации, образованию и средствам, необходимым им для того, чтобы защитить себя. Чтобы добиться качественного

изменения в поведении населения, мы подготовим набор четких и согласованных рекомендаций по кибербезопасности, которые будут предоставляться от имени Правительства и наших партнеров. NCSC будет предоставлять технические консультации, которые послужат основой для этих рекомендаций. В них будут отражены приоритеты и практические правила для бизнеса и населения — четкие, доступные, последовательные и в то же время актуальные с точки зрения существующих угроз. Правоохранительные органы будут тесно сотрудничать с представителями отрасли и NCSC в целях обмена информацией об актуальных криминальных угрозах и поддержки деятельности по защите от угроз и смягчению последствий для британского населения и организаций, пострадавших от атак.

Измерение успеха

5.5.6. Правительство будет измерять успех своей деятельности по защите КНИ и других приоритетных секторов путем оценки прогресса в достижении следующих результатов:

- уровень безопасности британской экономики сопоставим с уровнем кибербезопасности в развитых странах или превышает его;
- количество, серьезность и последствия успешных кибератак на компании в Великобритании сократились в результате улучшения и соблюдения элементарных правил;
- культура кибербезопасности улучшилась в масштабах всей Великобритании в результате того, что организации и население понимают существующие кибер-риски и знают, что необходимо делать для управления ими.

CYBER AWARE

Кампания Cyber Aware (бывшая Cyber Streetwise) предоставляет гражданам необходимые рекомендации по защите от киберпреступников. Целевое информирование через социальные сети и рекламу, осуществляемые в партнерстве с бизнесом, продвигает следующие идеи:

- использование трех случайных слов для создания надежных паролей;
- необходимость всегда загружать последние обновления программного обеспечения.

Эксперты соглашаются с тем, что эти действия обеспечат защиту небольших компаний и отдельных лиц от киберпреступлений. Cyber Aware
в настоящее время пользуется поддержкой со стороны 128 межотраслевых партнеров, в том числе полиции и компаний, работающих в секторах розничной торговли, досуга, туризма и услуг профессионального характера. В 2015-2106 гг. примерно 100 млн взрослого населения и 1 млн небольших компаний заявило, что с более высокой вероятностью будут выполнять основные действия по обеспечению кибербезопасности в результате воздействия кампании Cyber Aware.

Подробнее см. на сайте cyberaware.gov.uk

CYBER ESSENTIALS

Программа Cyber Essentials была разработана с тем, чтобы продемонстрировать организациям, как следует защищаться от «массовых атак» низкого уровня. Она перечисляет пять элементов технического контроля (контроль доступа; межсетевой экран периметра и интернет-шлюзы; защита от вредоносного ПО; управление исправлениями и защищенная конфигурация), которые должна обеспечить каждая организация. В преимущественном большинстве кибератак применяются относительно простые методы, использующие элементарные уязвимости ПО и компьютерных систем. Некоторые средства и инструменты находятся в открытом доступе в интернете, что позволяет даже дилетантам использовать эти уязвимости. Надлежащее исполнение рекомендаций программы Cyber

Essentials поможет защититься от основного числа распространенных атак через интернет.

5.6. УПРАВЛЕНИЕ ПРОИСШЕСТВИЯМИ И ПОНИМАНИЕ УГРОЗ

5.6.1. Число и серьезность кибер-происшествий, затрагивающих организации государственного и частного сектора, с большой вероятностью возрастут. Поэтому необходимо определить, каким образом организации как частного, так и государственного сектора будут взаимодействовать с Правительством в случае кибер-происшествия. Мы четко обозначим уровень поддержки каждого сектора — принимая во внимание уровень развития кибербезопасности в них — со стороны правительства и обеспечим их понимание со стороны организаций. Сбор и распространение Правительством информации об угрозах должны осуществляться такими путями и такими темпами, которые являются приемлемыми для всех типов организаций. Представители частного сектора, правительства и населения в настоящее время имеют доступ к целому ряду источников информации, рекомендаций и помощи в области кибербезопасности. Это необходимо упростить.

5.6.2. Мы должны обеспечить, чтобы деятельность Правительства в контексте как реагирования на происшествия, так и предоставления рекомендаций, осуществлялась не в изоляции, а в партнерстве с частным сектором. Наши процессы управления происшествиями должны отражать целостный подход к реагированию на них, позволяя нам перенимать опыт партнеров и обмениваться информацией о приемах смягчения последствий. Мы и далее будем поддерживать отношения с другими группами реагирования на чрезвычайные происшествия в области компьютерной безопасности (CERT) и нашими союзниками в рамках деятельности по управлению происшествиями.

5.6.3. В настоящее время управление происшествиями остается несколько фрагментированным и распределено между различными правительственными департаментами, и эта стратегия призвана разработать унифицированный подход. NCSC оптимизирует управление реагированием на происшествия, осуществляемое под эффективным руководством правительства. В случае крупной кибератаки мы обеспечим способность наших Вооруженных сил предоставлять поддержку, будь то в традиционной форме — ликвидируя физические последствия происшествия, или в форме специализированной поддержки со стороны киберперсоанала регулярных или резервных формирований. Правительство будет оказывать помощь, используя все имеющиеся ресурсы, при этом подчеркивая важность соблюдения элементарных правил кибербезопасности со стороны предприятий, общества и населения.

Цели

5.6.4. Мы преследуем следующие цели:

- Правительство разработает единый и согласованный подход к управлению происшествиями, основанный на углубленном понимании угроз и действий, направленных против нас, и повышения уровня осведомленности о них. NCSC будет основной движущей силой, наряду с партнерами из частного сектора, правоохранительных органов и других правительственных департаментов, органов и ведомств;
- NCSC определит четкие процедуры информирования о происшествиях, адаптируемые с учетом особенностей пострадавшего лица или организации;
- мы будем предупреждать самые распространенные кибер-происшествия и внедрим эффективные структуры обмена информацией для распространения сведений о планировании предупредительных мер.

Наш подход

5.6.5. Ответственность за обеспечение безопасности сетей и реализацию планов реагирования на происшествия возлагается на руководство организаций и компаний как частного, так и государственного сектора. На случай значительных происшествий Правительством разработан порядок управления происшествиями, отражающий три основных элемента кибер-происшествий: исходные причины, само происшествие и действия по факту происшествия.

5.6.6. Чтобы управление происшествиями было эффективным как для правительства, так и для частного сектора, мы будем осуществлять, совместными усилиями, анализ и определения объема ответных действий правительства, чтобы обеспечить укрепление сотрудничества. Мы будем развивать национальный план киберучений на основе более глубокого понимания и осознания угрозы, чтобы усовершенствовать поддержку, оказываемую нами партнерам из государственного и частного сектора.

5.6.7. Мы сделаем правительство авторитетным и надежным источником рекомендаций, помощи и поддержки. Это повысит уровень осведомленности о кибербезопасности в масштабах всего британского «цифрового сообщества» и расширит наши возможности по определению тенденций, принятию инициативных мер и, в конечном итоге, предотвращению инцидентов.

5.6.8. С переходом к автоматизированному обмену информацией (при котором системы кибербезопасности автоматически отправляют друг другу уведомления о происшествиях или атаках) мы обеспечим более эффективное обслуживание. Это позволит организациям оперативно принимать меры с учетом соответствующей информации об угрозах.

Измерение успеха

5.6.9. Правительство будет измерять успех своей деятельности по управлению происшествиями путем оценки прогресса в достижении следующих результатов:

- увеличивается доля происшествий, о которых пострадавшие сообщают в органы власти, что позволяет лучше понять размер и масштаб угрозы;
- в результате создания NCSC в качестве централизованного механизма сбора информации об угрозах и реагирования на атаки осуществляется более эффективное и комплексное управление киберугрозами;
- мы работаем над искоренением основных причин атак на национальном уровне, сокращая число случаев повторного использования уязвимостей в системах различных пользователей и секторов.

6. СДЕРЖИВАНИЕ

6.0.1. В Стратегии национальной безопасности говорится, что оборона и защита начинаются с сдерживания. Это в равной степени относится и киберпространству. Для воплощения в жизнь нашего видения нации, надежно защищенной и устойчивой к киберугрозам, процветающей и уверенно пользующейся цифровыми технологиями, мы должны отвратить и сдержать действия тех, кто может нанести урон нам и нашим интересам. Для достижения этого мы все должны и далее работать над повышением уровней кибербезопасности, чтобы атаковать на нас в киберпространстве — будь то с целью хищения или нанесения урона — было недешево и непросто. Наши противники должны знать, что их действия не останутся безнаказанными: мы можем их установить, и непременно установим, их личности, а также в состоянии предпринять действия против них, обращаясь к самым подходящим средствам реагирования из арсенала орудий, имеющихся в нашем распоряжении. Мы продолжим объединяться с союзниками на международном уровне и продвигать применение международных законов в киберпространстве. Мы также будем более активно срывать деятельность всех тех, кто угрожает нам в киберпространстве, и разрушать инфраструктуру, на которую они полагаются. Для достижения этих масштабных планов нам потребуются суверенные возможности.

6.1. РОЛЬ КИБЕРБЕЗОПАСНОСТИ В СДЕРЖИВАНИИ

6.1.1. Киберпространство является лишь одной из сфер, в которых мы должны защищать свои интересы и суверенитет. Так же как наши действия в физическом пространстве связаны с кибербезопасностью и сдерживанием, так и наши действия и позиции в киберпространстве должны содействовать национальной безопасности в целом.

6.1.2. Принципы сдерживания одинаково применимы и к киберпространству, и физическому пространству. Великобритания четко дает понять, что для сдерживания противников и лишение их возможностей для атаки на нас будет применяться весь спектр наших возможностей. Однако мы понимаем, что кибербезопасность и устойчивость сами по себе являются средствами сдерживания атак, которые полагаются на использование уязвимостей.

6.1.3. Мы разработаем комплексный подход к кибербезопасности и сдерживанию на национальном уровне, который поможет сделать Великобританию более трудным объектом для нападения за счет уменьшения выгод и увеличения затрат любого противника в любой области — политической, дипломатической, экономической или стратегической. Мы сможем влиять на решения потенциальных противников, если дадим им понять, что у нас есть возможности и намерения решительно реагировать на атаки. У нас будут необходимые средства и потенциал, чтобы: лишить наших противников простых возможностей для нарушения безопасности наших сетей и систем; чтобы понять их намерения и возможности; чтобы противостоять угрозе широкомасштабного использования массового вредоносного ПО и чтобы предпринять ответные действия и защитить нацию в киберпространстве.

6.2. СОКРАЩЕНИЕ УРОВНЯ КИБЕРПРЕСТУПНОСТИ

6.2.1. Необходимо обеспечить возрастание издержек, увеличение рисков и уменьшение вознаграждений в связи с киберпреступной деятельностью. На фоне укрепления защиты Великобритании от кибератак и уменьшения количества уязвимостей мы также должны неустанно преследовать преступников, которые продолжают атаковать Великобританию.

6.2.2. Правоохранительные органы должны сосредоточить усилия на преследовании преступников, которые упорно продолжают атаковать британских граждан и бизнес. Мы

будем сотрудничать с отечественными и международными партнерами в преследовании преступников, где бы они ни находились, и в разрушении их инфраструктуры и сетей поддержки. Правоохранительные органы, в сотрудничестве с NCSC, также продолжат работу по повышению уровня осведомленности и стандартов кибербезопасности.

6.2.3. Настоящая стратегия дополняет Стратегию противодействия особо опасной и организованной преступности, в которой изложены стратегические меры реагирования на киберпреступность, равно как и на другие виды особо опасной и организованной преступности. Национальный отдел расследования киберпреступлений (NCCU) в структуре Национального агентства по борьбе с преступностью (NCA) призван осуществлять руководство и координацию деятельности по реагированию на киберпреступления на национальном уровне. Action Fraud — национальный центр сбора информации о мошенничествах и киберпреступлениях. Сеть подразделений по борьбе с киберпреступностью в рамках Региональных отделов по борьбе с организованной преступностью (ROCU) обеспечивает доступ к специализированным средствам противодействия киберпреступлениям на региональном уровне и поддерживает работу NCCU и местных сил.

Цель

6.2.4. Мы сократим последствия киберпреступной деятельности для Великобритании и ее интересов, сдерживая киберпреступников от атак на цели в Великобритании и неустанно преследуя тех, кто продолжает атаковать нас.

Наш подход

6.2.5. В целях сокращения последствий киберпреснупной деятельности мы будем:

• наращивать потенциал и повышать уровень возможностей и квалификаций в британских правоохранительных органах на национальном, региональном и местном уровнях в целях выявления, преследования, привлечения к ответственности и сдерживания киберпреступников в Великобритании и за рубежом;
• углублять понимание бизнес-моделей киберпреступности, что позволит нам применять ответные действия там, где это даст наибольший эффект в контексте ее пресечения. Мы используем эти знания для того, чтобы:

- создать в Великобритании такие условия, при которых киберпреступная деятельность будет высоко затратной и сопряженной с высокой степенью риска, направляя усилия на разрыв порочного круга преступности и, совместно с представителями отрасли, уменьшая способность преступников использовать уязвимости британской инфраструктуры;
- подавлять преступность в зародыше, нарушая криминальную бизнес-модель путем разрушения ее инфраструктуры и финансовых сетей, и, где это возможно, привлечения преступников к ответственности.

• создавать международные партнерства, чтобы положить конец кажущейся безнаказанности киберпреступников, действующих против Великобритании, привлекая их к ответственности в зарубежных юрисдикциях;
• отвращать людей от участия или вовлечения в киберпреступность с помощью мер раннего вмешательства;
• расширять сотрудничество с представителями отрасли, предоставляя в их распоряжение упреждающую информацию об угрозах

и получая от них информацию о готовящихся атаках, которая у них есть, что поможет нам подавлять преступность в зародыше;
• разработаем систему круглосуточного сбора и сортировки информации в структуре Action Fraud, которая будет связана с NCSC, Национальным отделом расследования киберпреступлений при NCA и правоохранительными органами в целом, с тем, чтобы улучшить поддержку пострадавшим от киберпреступности, оперативнее реагировать на сообщения о преступлениях и рекомендации по укреплению безопасности. Будет создана новая система информирования, способствующая обмену информацией о киберпреступлениях и угрозах в режиме реального времени в масштабах всей правоохранительной отрасли;
• сотрудничать с NCSC и представителями частного сектора в целях сокращения количества уязвимостей в британской инфраструктуре, которые могут быть использованы киберпреступниками в достаточно больших масштабах;
• сотрудничать с представителями финансового сектора с тем, чтобы создать в Великобритании неблагоприятные условия для деятельности по монетизации похищенных идентификационных данных, в том числе по разрушению криминальных сетей.

Измерение успеха

6.2.6. Правительство будет измерять успех своей деятельности по сокращению киберпреступности путем оценки прогресса в достижении следующих результатов:

• повысилась результативность деятельности по пресечению кибер-атак на Великобритании, в том числе увеличилось число арестов и обвинительных приговоров и было уничтожено больше криминальных сетей в результате действий правоохранительных органов;
• улучшены возможности правоохранительных органов, в том числе расширен потенциал и повысился уровень квалификаций специалистов и персонала в общем, а также расширены правоохранительные возможности наших зарубежных партнеров;
• повысилась эффективность и масштабность мер раннего воздействия, направленных на отвращение от криминальной деятельности и перевоспитание правонарушителей;
• в результате того, что затруднился доступ к криминальным кибер-услугам и снизилась их эффективность, сократилось число киберпреступлений низкого уровня.

ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ КИБЕРПРЕСТУПЛЕНИЯ

Если у рядового гражданина есть основания полагать, что он стал жертвой киберпреступления или мошенничества, совершенного в киберпространстве, следует обратиться в организацию Action Fraud.

Сообщить о происшествии можно через интернет с помощью системы сообщения о мошенничестве Action Fraud в любое время суток или по телефону 0300 123 2040. Дополнительную информацию см. на сайте www.actionfraud.police.uk

Служба Action Fraud находится в ведении полиции Лондонского сити.

6.3. ПРОТИВОДЕЙСТВИЕ ВРАЖДЕБНЫМ ИНОСТРАННЫМ СУБЪЕКТАМ

6.3.1. Мы должны направлять все возможности, имеющиеся в распоряжении правительства, на противодействие атакам со стороны враждебных иностранных субъектов,

которые все чаще угрожают нашей политической, экономической и военной безопасности. Ключевое значение для нашего успеха будет иметь сотрудничество с международными партнерами. Мы будем прикладывать больше усилий для вовлечения их в нашу работу и сотрудничество в области противодействия угрозам. Больший объем этой деятельности будет осуществляться за рамками общественного внимания. Инвестиции в развитие суверенных возможностей и партнерских отношений с представителями отрасли и частного сектора будут способствовать дальнейшему укреплению нашей способности к обнаружению, отслеживанию и распознаванию постоянно эволюционирующей деятельности, направленной против нас.

Цель

6.3.2. Будут разработаны стратегии, политики и приоритеты в отношении каждого противника с тем, чтобы мы могли применять упреждающий, тщательно выверенный и эффективный подход к противодействию угрозам, а также сокращению числа и уменьшению уровня опасности кибер-происшествий.

Наш подход

6.3.3. Для сокращения угрозы со стороны враждебных иностранных субъектов мы будем:

- содействовать применению международных законов в киберпространстве в дополнение к продвижению договоренности о добровольных, необязывающих нормах ответственного поведения со стороны государств, а также разработке и внедрению мер по укреплению доверия;
- сотрудничать с международными партнерами, прежде всего, в области коллективной обороны, общей безопасности и более активного сдерживания противника, в пределах нашего членства НАТО;
- выявлять индивидуальные и общие аспекты деятельности наших противников в киберпространстве;
- развивать и изучать доступные пути сдерживания и противодействия этой угрозе, опираясь на весь спектр возможностей государства. Мы примем во внимание другие факторы, связанные с этой деятельностью, в том числе стратегии по отдельным странам, приоритеты международной кибердеятельности, а также цели в области противодействия киберпреступности и обеспечения благосостояния;
- будем использовать существующие сети и взаимосвязи с ключевыми международными партнерами для обмена информацией о текущих и зарождающихся угрозах, дополняя существующие знания и опыт;
- публично раскрывать личности ответственных за кибер-атаки, если это, по нашему мнению, отвечает национальным интересам.

Измерение успеха

6.3.4. Правительство будет измерять успех своей деятельности по противодействию враждебным иностранным субъектам путем оценки прогресса в достижении следующих результатов:

- укрепление сетей, учрежденных нами для обмена информацией с международными партнерами, и расширение многосторонних соглашений, утверждающих законное и ответственное поведение со стороны государств, помогают нам лучше понять угрозы, реагировать на них и в конечном итоге укрепить оборону Великобритании;
- в результате принятия мер по укреплению обороны и сдерживанию, наряду с разработкой стратегий по отдельным странам, созданы условия, в

которых враждебным иностранным субъектам трудно атаковать Великобританию.

6.4. ПРЕДУПРЕЖДЕНИЕ ТЕРРОРИЗМА

6.4.1. Текущие технические возможности террористов все еще являются ограниченными, но они продолжают вынашивать планы по нападению на компьютерные сети Великобритании, главной целью которых является широкое освещение в прессе и саботаж. Правительство будет работать над выявлением личностей террористов, использующих и намеревающихся использовать киберпространство для своих целей, и пресечением их деятельности. Таким образом мы сведем к минимуму последствия их деятельности и предупредим развитие возможностей для террористический действий в киберпространстве, которые могли бы составить угрозу британским сетям и национальной безопасности.

Цель

6.4.2. Смягчение угрозы использования киберпространства в террористических целях путем установления личностей и срыва деятельности кибер-террористов, которые уже имеют, или планируют получить возможности, способные составить угрозу для национальной безопасности Великобритании.

Наш подход

6.4.3. Для сохранения низкого уровня угрозы кибер-терроризма, мы будем:

- осуществлять деятельность по обнаружению угроз кибер-терроризма, устанавливая личности субъектов, планирующих операции по выводу из строя сетей Великобритании и союзных стран;
- расследовать и пресекать действия кибер-террористов с тем, чтобы лишить их возможности осуществления кибер-деятельности против Великобритании и ее союзников;
- тесно сотрудничать с международными партнерами с тем, чтобы эффективнее противостоять угрозе кибер-терроризма.

Измерение успеха

6.4.4. Правительство будет измерять успех своей деятельности по предупреждению терроризма путем оценки прогресса в достижении следующих результатов:

- достигнуто полное понимание рисков, которые несет в себе кибер-терроризм, путем установления личностей террористов и расследования угроз кибер-терроризма в Великобритании;
- обеспечен мониторинг и срыв террористической деятельности в киберпространстве при первой возможности с целью предотвращения наращивания такого террористического потенциала в долгосрочной перспективе.

6.5. РАСШИРЕНИЕ СУВЕРЕННЫХ ВОЗМОЖНОСТЕЙ – НАСТУПАТЕЛЬНЫЕ КИБЕРОПЕРАЦИИ

6.5.1. Возможности для наступательных кибероперациий предусматривают намеренное вмешательство в системы и сети противников с целью их повреждения, дестабилизации и разрушения. Наступательные действия в киберпространстве являются одной из целого спектра возможностей, разрабатываемых нами для сдерживания противников и лишения их возможностей для нападения на нас как в кибернетическом, так и в физическом пространстве. Национальной программой наступательных кибероперациий (NOCP) предусмотрен специализированный функционал для действий в киберпространстве, и мы выделим ресурсы на его разработку и усовершенствование.

Цель

6.5.2. Мы должны иметь в нашем распоряжении арсенал возможностей для наступательных действий в киберпространстве, готовый к использованию по необходимости в целях сдерживания и противодействия в соответствии с национальным и международным законодательством.

Наш подход

6.5.3. В этих целях мы будем:

- вкладывать средства в программу NOCP, осуществляемую в партнерстве между министерством обороны и GCHQ с использованием специалистов и экспертов обеих организаций и направленную на разработку необходимого инструментария, приемов и методов;
- развивать способность использования инструментальных средств для наступательных действий в киберпространстве;
- развивать способность Вооруженных сил к развертыванию наступательных действий в киберпространстве как неотъемлемую часть их операций, тем самым усиливая общую результативность военных действий.

Измерение успеха

6.5.4. Правительство будет измерять успех своей деятельности по созданию функциональных возможностей для наступательных кибероперациий путем оценки прогресса в достижении следующих результатов:

- Великобритания является одним из мировых лидеров по возможностям для наступательных кибероперациий;
- Великобритания создала канал подготовки квалифицированных кадров, необходимых для разработки и развертывания суверенных возможностей в киберпространстве.

6.6. РАСШИРЕНИЕ СУВЕРЕННЫХ ВОЗМОЖНОСТЕЙ – КРИПТОГРАФИЯ

6.6.1. Криптографические возможности имеют фундаментальное значение для защиты самой секретной информации и решений о развертывании Вооруженных сил и использовании потенциала национальной безопасности. Для сохранения этой способности нам необходимы знания, умения и технологии частного сектора, проверенные GCHQ. Эта деятельность, очевидно, должна осуществляться на территории Великобритании с привлечением британских граждан, имеющих необходимый допуск и работающих в компаниях, готовых открыто и подробно обсуждать с GCHQ вопросы проектирования и внедрения решений. МО и GCHQ работают над тем, чтобы оценить резонный объем долгосрочных издержек, связанных с сохранением суверенных криптографических средств, ориентируясь на превалирующие рыночные условия и в сотрудничестве с компаниями, которые уже способны поставить такие решения.

Цель

6.6.2. Мы уверены в том, что Великобритания будет всегда сохранять политический контроль над криптографическими средствами, имеющими критическое значение для национальной безопасности, и, следовательно, для защиты британских секретов.

Наш подход

6.6.3. Мы отдадим предпочтение средствам, которые позволят нам эффективно обмениваться информацией с нашими союзниками и обеспечить доступность надежной информации и информационных систем при первой необходимости. Тесно сотрудничая с другими государственными департаментами и ведомствами, GCHQ и МО определят суверенные требования и наилучшие способы удовлетворения этих

требований с учетом того, что поставщики должны быть отечественными компаниями. Эта работа будет осуществляться в рамках новой общей структуры, которая будет использоваться для определения требований, необходимых для обеспечения операционного преимущества и свободы действий.

Измерение успеха

6.6.4. Правительство будет измерять успех своей деятельности по сохранению криптографических функциональных возможностей путем оценки прогресса в достижении следующего результата:

- наши суверенные криптографические возможности являются эффективными в контексте защиты тайн и секретной информации от несанкционированного раскрытия.

ШИФРОВАНИЕ

Шифрование — это процесс кодирования данных или информации с целью предупреждения несанкционированного доступа к ним.

Правительство поддерживает идею шифрования. Шифрование является основой для крепкой экономики на базе интернета: оно обеспечивает защиту персональных данных и интеллектуальной собственности и гарантирует безопасность электронной коммерции.

Однако по мере эволюции технологий мы должны обеспечивать отсутствие гарантированно «безопасных территорий» для деятельности террористов и преступников, которые находятся вне досягаемости законов.

Принимая во внимание развитие технологий, Правительство стремится наладить сотрудничество с представителями отрасли с тем, чтобы обеспечить, что при наличии прочной законодательной базы и прозрачного контроля, полиция и разведывательные органы смогут получать доступ к содержимому коммуникаций террористов и преступников. Существующее законодательство позволяет перехватывать коммуникации преступников и террористов при наличии соответствующего ордера. Компании обязаны подчиняться требованию такого ордера и предоставлять компетентным органам доступ к затребованным коммуникациям. При вручении ордера компаниям выдвигают требование снять шифрование, примененное ими или от их имени, чтобы предоставленные материалы были доступны для чтения. Согласно закону, компании обязаны предпринимать разумные действия для выполнения требования ордера, и при оценке «разумности» будет учитываться оценка действий по снятию шифрования, которые компания обязана выполнить.

7. РАЗВИТИЕ

7.0.1. В разделе стратегии «РАЗВИТИЕ» описывается, каким образом мы будем приобретать и укреплять инструментальные средства и возможности, необходимые Великобритании для защиты от кибер-угроз.

7.0.2. Великобритании требуются более квалифицированные и талантливые специалисты по кибербезопасности. Правительство будет принимать меры уже сегодня, чтобы устранить пробел между спросом и предложением на рынке ключевых специалистов по кибербезопасности, и активизирует работу в области образования и подготовки таких специалистов. Это долгосрочная, трансформационная цель, и настоящая стратегия положит начало важной работе в этой области, которая непременно продолжится и после 2021 г. Квалифицированная рабочая сила — источник жизненной силы для ведущей в мире коммерческой экосистемы кибербезопасности. Эта экосистема призвана обеспечить успех и необходимую поддержку стартапов в области кибербезопасности. Такой уровень инновационной и активной деятельности возможен только в частном секторе; однако Правительство будет поддерживать ее развитие и активно продвигать сектор кибербезопасности на мировом рынке. Для развития потенциала квалифицированных кадров, равно как и для претворения новых идей в технически совершенные продукты, требуется динамичный и процветающий сектор научных исследований.

7.1. УКРЕПЛЕНИЕ КАДРОВОГО ПОТЕНЦИАЛА В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

7.1.1. Великобритания должна решить системные проблемы, лежащие в основе дефицита специалистов в кибернетической области: недостаточное количество молодых людей, выбирающих эту профессию; недостаток имеющихся специалистов по кибербезопасности; недостаточное освещение концепций кибернетической и информационной безопасности в программах компьютерных курсов; нехватка квалифицированных преподавателей; и отсутствие канала карьерного роста и подготовки для этой профессии.

7.1.2. Это обуславливает необходимость неотложного вмешательства со стороны Правительства с целью преодоления текущего дефицита кадров и разработки согласованной долгосрочной стратегии по устранению этих пробелов на основании уже предпринятых действий. Однако необходимо признать, что для достижения значимого эффекта требуются коллективные усилия при участии широкого ряда авторитетных лиц и организаций в масштабах Правительств Шотландии, Уэльса и Северной Ирландии, государственного сектора, образовательных учреждений, научных кругов и предприятий.

Цель

7.1.3. Конечная цель Правительства — обеспечить стабильную подготовку отечественных кадров, компетентных в области кибербезопасности, на фоне финансирования специфических мер по устранению дефицита квалифицированных кадров в краткосрочной перспективе. Мы также определим и будем развивать среди населения и рабочей силы навыки кибербезопасности, необходимые для безопасного пользования Интернетом.

7.1.4. Для этого необходимо осуществлять деятельность в течение следующих не пяти, а двадцати лет. Мы определим набор долгосрочных, скоординированных мер, которые должны принять правительственные органы, предприятия, образовательные учреждения и научные организации, для того чтобы обеспечить стабильную подготовку специалистов по кибербезопасности, отвечающих необходимым стандартам, должным образом сертифицированных и способных работать уверенно и безопасно.

7.1.5. Мы устраним дефицит квалифицированных кадров в области обороны. Мы привлечем к работе в правительстве специалистов, которые не только имеют хорошую подготовку, но и готовы работать над сохранением национальной безопасности. Сюда входит понимание воздействия, которое киберпространство оказывает на военные операции.

Наш подход

7.1.6. Мы разработаем и внедрим автономную стратегию повышения квалификации, опираясь на достигнутые результаты работы по интеграции программы кибербезопасности в систему образования. Это позволит далее улучшить состояние дел в преподавании компьютерных наук в целом и интегрировать вопросы кибербезопасности в программу обучения. Каждый человек, изучающий компьютерные науки, технологии или совершенствующий свои цифровые навыки, будет изучать основы кибербезопасности и сможет использовать полученные знания в своей работе. В рамках этой деятельности мы обратим внимание на гендерный дисбаланс в кибер-ориентированных профессиях и будем стремиться охватить разнообразные группы населения, чтобы как можно больше расширить выбор талантливых специалистов. Мы будем тесно сотрудничать с Правительствами Шотландии, Уэльса и Северной Ирландии, чтобы обеспечить единообразие подхода в масштабах всей Великобритании.

7.1.7. Мы более четко сформулируем обязанности правительства и отрасли, с учетом их возможного изменения с течением времени. Британское Правительство и Правительства Шотландии, Уэльса и Северной Ирландии играют ключевую роль в создании условий, необходимых для повышения квалификаций и укрепления навыков в области кибербезопасности, а также в модернизации системы образования с учетом изменяющихся потребностей отрасли и правительства. При этом работодатели со своей стороны обязаны четко формулировать свои потребности, а также обеспечивать подготовку и развитие своих сотрудников и молодых людей, выбирающих эти профессии. Важная роль в этом процессе отводится представителям отрасли, которые, совместно с научными кругами, профессиональными органами и отраслевыми объединениями, должны создавать привлекательные условия для карьерного роста и дальнейшего обучения.

7.1.8. Признавая, что перед нами стоит общая задача по устранению дефицита квалифицированных кадров, мы сформируем специальную консультативную группу, в которую войдут представители правительства, работодателей, профессиональных органов, сертификационных организаций, образовательных учреждений и научных кругов. Это укрепит согласованность деятельности в ключевых секторах. Эта группа поддержит разработку долгосрочной стратегии, которая будет учитывать достижения в области широкого спектра цифровых квалификаций и обеспечивать ее согласование с соображениями кибербезопасности и их интеграцию. Эта группа будет сотрудничать с аналогичными органами по всей Великобритании.

7.1.9. Помимо работы в этом направлении, Правительство будет вкладывать средства в реализацию ряда инициатив, направленных на немедленное улучшение состояния дел в этой области и получение информации, необходимой для разработки долгосрочной стратегии развития кадрового потенциала. Среди них:

- разработка школьной программы, нацеленной на качественное преобразование преподавания кибербезопасности и подготовки талантливых 14-18-летних учащихся (включая классные занятия, внешкольные занятия с опытными

менторами, интересные проекты и летние школы)
• организация стажировки для выпускников институтов и университетов в организациях энергетического, финансового и транспортного секторов, с целью устранения пробелов в умениях и знаниях в важных областях;
• образование фонда переподготовки кандидатов из числа сотрудников, которые уже работают в организации и имеют качества, необходимые для специалистов по кибербезопасности;
• выявление и поддержка качественных программ в области кибербезопасности на уровне высшего и последипломного образования, а также выявление и устранение дефицита специалистов во всех областях с признанием ключевой роли университетов в их подготовке;
• поддержка процесса аккредитации профессионального развития преподавателей в области кибербезопасности. Это должно помочь преподавателям и другим специалистам лучше понять особенности преподавания кибербезопасности и будет использоваться для аккредитации специалистов в этой области;
• формирование профессии специалиста по кибербезопасности, в том числе путем присвоения Королевского Диплома до 2020 г., обеспечивающего отраслевое признание организации высококвалифицированных специалистов по кибербезопасности и централизацию усилий по консультированию, формированию и информированию национальной политики;
• формирование Академии кибероборонь в качестве центра передового опыта в области обучения и подготовки специалистов по кибербезопасности для Министерства обороны и других государственных учреждений, что улучшит подготовку профессиональных кадров и образование в целом;
• развитие возможностей для сотрудничества между государственными учреждениями, Вооруженными силами, предприятиями и научными организациями в области подготовки и образования, а также создание условий для отработки и сохранения полученных знаний и навыков;
• мы будем сотрудничать с отраслевыми предприятиями в области расширения сферы действия программы CyberFirst на подбор и подготовку молодых талантливых специалистов из различных слоев общества для работы в области защиты национальной безопасности;
• интеграция изучения кибербезопасности и навыков работы с цифровыми технологиями в обучающие программы на всех уровнях системы образования — от начальной школы до последипломного обучения, — установление стандартов, повышение качества обучения и создание твердых основ для дальнейшего карьерного роста в этой отрасли.

Образование входит в сферу ответственности Правительств Шотландии, Уэльса и Северной Ирландии, и некоторые из этих инициатив относятся, главным образом, к Англии. В этой связи мы будем сотрудничать с Правительствами Шотландии, Уэльса и Северной Ирландии, чтобы обеспечить единообразие подхода в масштабах всех систем образования Великобритании.

Измерение успеха

7.1.10. Правительство будет измерять успех своей деятельности по укреплению кадрового потенциала в области кибербезопасности путем оценки прогресса в достижении следующих результатов:

• существуют действенные и четко обозначенные пути выбора профессии специалиста по кибербезопасности,

привлекательные для широкого круга людей;
• к 2021 г. кибербезопасность практически стала неотъемлемой составляющей соответствующих программ обучения на всех уровнях — от начальной школы до последипломного обучения;
• профессия специалиста по кибербезопасности утвердилась, получила широкое признание и Королевский Диплом, оформились пути карьерного роста;
• изучение кибербезопасности в определенном объеме вошло в программы повышения квалификации соответствующих работников, не специализирующихся на кибербезопасности, в масштабах всей экономики;
• Правительство и Вооруженные силы имеют доступ к специалистам по кибербезопасности, способным поддерживать безопасность и устойчивость Великобритании к угрозам.

7.2. СТИМУЛИРОВАНИЕ РОСТА СЕКТОРА КИБЕРБЕЗОПАСНОСТИ

7.2.1. Для современной, цифровой экономики требуется быстро растущий и инновационный сектор кибербезопасности. Британские фирмы, работающие в отрасли кибербезопасности, поставляют ведущие в мире технологии и услуги по обучению и консалтингу для бизнеса и правительства. И хотя Великобритания играет роль лидера в этой области, чтобы оставаться впереди, она должна обогнать серьезных конкурентов. Существуют также барьеры, которые предстоит преодолеть Правительству. Британские компании и ученые разрабатывают передовые технологии, но некоторым из них требуется поддержка в развитии коммерческих и предпринимательских навыков, необходимых для их выживания. В силу недостатка финансирования малые и средние предприятия не могут развиваться и выходить на новые рынки и территории. Некоторые компании, разрабатывающие самые революционные продукты и услуги, способные помочь нам опережать развитие угроз, затрудняются найти заказчиков, которые бы согласились выступить в роли первых пользователей. Для преодоления этих вызовов требуется совместная работа представителей правительства, отрасли и научных организаций.

Цель

7.2.2. Правительство будет поддерживать создание растущего, инновационного и процветающего сектора кибербезопасности в Великобритании, чтобы создать такую экосистему, где:

• компании, специализирующиеся на безопасности, будут преуспевать и привлекать инвестиции, необходимые для их роста;
• самые опытные специалисты из государственных учреждений, научных организаций и предприятий частного сектора будут совместно работать над ускорением инноваций;
• клиенты Правительства и отрасли готовы к использованию самых передовых услуг и достаточно уверены в них.

Наш подход

7.2.3. С целью создания такой экосистемы мы:

• выведем научные инновации в коммерческое обращение, организуя соответствующую подготовку и курирование ученых;
• откроем два инновационных центра, нацеленных на разработку передовых киберпродуктов и развитие новых, динамичных компаний по кибербезопасности, которые составят основу для реализации программы инициатив, призванных помочь

стартапам с привлечением первых клиентов и дальнейших инвестиций.
• выделим часть средств из Фонда обороны и инноваций в кибернетике объемом 165 млн фунтов на закупку инновационных продуктов на нужды обороны и безопасности;
• предоставим компаниям испытательную базу, необходимую для разработки продуктов, и средства ускоренной оценки нового поколения продуктов и услуг в области кибербезопасности по мере их создания, что позволит клиентам уверенно пользоваться ими;
• будем опираться на коллективный опыт, накопленный в рамках Cyber Growth Partnership (партнерства между отраслью и правительством), в работе по формированию и направлению дальнейшего роста и внедрению инноваций;
• будем помогать компаниям, независимо от размера, расширять деятельность и выходить на международные рынки;
• будем содействовать установлению международной договоренности о стандартах, которые повышают доступность британского рынка.

7.2.4. Мы также будем использовать государственные закупки товаров и услуг для стимулирования инноваций. В области кибербезопасности перед Правительством стоят наиболее серьезные вызовы и самые большие угрозы. Мы можем и мы должны найти самые эффективные решения этих проблем. Для этого необходимо упростить ведение бизнеса с государством для небольших компаний. Для этого Правительство должно принять менее осторожный подход к испытанию и использованию новых продуктов. Это взаимовыгодное решение: правительство получит доступ к лучшим услугам, а производители инновационных технологий получат первых пользователей, что облегчит для них привлечение инвестиций и расширение клиентской базы. Мы будем поощрять все ветви правительства, в том числе Правительства Шотландии, Уэльса и Северной Ирландии, принять такой же подход.

«Мы стремимся создать экосистему, в которой стартапы в области кибертехнологий имели бы условия для быстрого роста и привлечения инвестиций, а также получали поддержку, необходимую для привлечения клиентов из разных стран мира и создания канала инноваций для обмена идеями между предприятиями частного сектора, правительством и научными организациями».

Достопочтенный Мэтт Хэнкок, член парламента,
Государственный министр по вопросам цифровых технологий и культуры

Измерение успеха

7.2.5. Правительство будет измерять успех своей деятельности по стимулированию роста сектора кибербезопасности путем оценки прогресса в достижении следующих результатов:

• достижение темпов ежегодного роста британского кибер-сектора, превышающих среднемировые;
• существенное увеличение объема инвестиций в молодые компании;
• внедрение инновационных и более эффективных технологий кибербезопасности в государственные системы.

7.3. СОДЕЙСТВИЕ РАЗВИТИЮ НАУКИ И ТЕХНОЛОГИИ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

7.3.1. В основе первоклассных возможностей Великобритании в области кибербезопасности лежит успешное развитие науки и технологий и передовые научно-исследовательские достижения. Для сохранения и укрепления репутации Великобритании как мирового лидера в области передовых исследований необходимо обеспечить, чтобы наши научно-

исследовательские учреждения продолжали привлекать лучших из лучших специалистов в области кибербезопасности. Для этого мы должны оказывать поддержку центрам передового опыта, которые привлекают самых способных и динамичных ученых и исследователей, а также углублять партнерские отношения между научными организациями, Правительством и отраслью. Для этого Правительство должно выступить в роли посредника, стимулирующего сотрудничество такого рода. В случае успеха мы создадим самообеспечивающуюся экосистему, поддерживающую свободное обращение идей — и передвижение людей — между тремя секторами с выгодой для каждого из них.

Цель

7.3.2. К 2021 г. Великобритания должна укрепить свое положение лидера в области кибернетических наук и технологий. Гибкие партнерские отношения между университетами и бизнесом будут способствовать превращению результатов научно-исследовательской деятельности в востребованные рынком продукты и услуги. Великобритания сохранит свою репутацию в области инноваций и передового опыта, в том числе в отраслях, гарантирующих национальную мощь, таких как финансовый сектор.

Наш подход

7.3.3. Для достижения этого Правительство будет поощрять сотрудничество, инновации, гибкие модели финансирования научной деятельности и вывод плодов научно-исследовательской деятельности в коммерческое обращение. Правительство обеспечит привлечение внимания к человеческим и поведенческим аспектам кибербезопасности и включение систем, выходящих за технические рамки, например бизнес-процессов и организационных структур, в сферу кибернетических наук и технологий.

7.3.4. Это ляжет в основу создания продуктов, систем и услуг, являющихся «безопасными по умолчанию», в которых соображения безопасности учитывались уже на этапе проектирования и для деактивации функций безопасности требуется осознанное решение пользователя.

7.3.5. Мы опубликуем подробную Стратегию развития кибернетических наук и технологий после проведения основательных консультаций с партнерами и заинтересованными сторонами. В рамках этой деятельности мы определим области науки и технологий, которые Правительство, представители отрасли и ученые считают важными, и выявим недостатки в возможностях, которые Великобритания имеет в настоящее время, с целью их устранения.

7.3.6. Правительство продолжит предоставлять финансирование и поддержку центрам передового академического опыта, научно-исследовательским институтам и докторантурам. Кроме того, мы откроем новые научно-исследовательские институты, занимающиеся стратегически важными тематиками. Мы также предоставим финансирование для осуществления дальнейших исследований в областях, в которых готовящаяся Стратегия развития кибернетических наук выявит недостатки возможностей. В число важных областей, которые могут получить финансирование, входят: аналитика больших данных, автономные системы, надежные промышленные системы управления, киберфизические системы и «интернет вещей», технологии «интеллектуального города», автоматизированная верификация систем и наука кибербезопасности.

7.3.7. Мы продолжим спонсировать обучение аспирантов, являющихся британскими гражданами, в центрах передового академического опыта, чтобы увеличить количество экспертов по кибербезопасности среди британских граждан.

7.3.8. Правительство будет работать с такими организациями, как Innovate UK и научно-исследовательские центры, в целях содействия сотрудничеству между отраслью, Правительством и научными организациями. В рамках поддержки такого сотрудничества мы изучим передовые методы в области присвоения категорий секретности и будем осуществлять подбор экспертов, включая ученых, имеющих допуск к секретным документам. Это позволит максимально расширить возможности коллективного подхода к работе как с несекретной, так и чрезвычайно секретной информацией.

7.3.9. Правительство будет финансировать программу «большого вызова», нацеленную на поиск и разработку инновационных решений для некоторых из самых жгучих проблем в области кибербезопасности. CyberInvest — новое партнерство между отраслью и Правительством, направленное на поддержку самых передовых исследований в области кибербезопасности и защиту Великобритании в киберпространстве — будет создано в рамках укрепления сотрудничества между научными кругами, правительством и отраслью.

Измерение успеха

7.3.10. Правительство будет измерять успех своей деятельности по содействию научно-технической деятельности в области кибербезопасности путем оценки прогресса в достижении следующих результатов:

- существенное увеличение числа британских компаний, достигших успеха в выводе в коммерческое обращение плодов научных исследований в области кибербезопасности, и сокращение недостатков научно-исследовательских возможностей в области кибербезопасности с эффективным их восполнением;
- Великобритания пользуется репутацией мирового лидера по исследованиям и инновациям в области кибербезопасности.

7.4. ЭФФЕКТИВНОЕ «СКАНИРОВАНИЕ ГОРИЗОНТОВ»

7.4.1. При формировании политики Правительство должно учитывать изменения кибернетического, геополитического и технологического ландшафта. В этой связи особое значение имеет эффективная работа по «сканированию горизонтов» и оценке угроз. Необходимо вкладывать средства в защиту от будущих угроз и предвосхищать изменения рынка, которые могут повлиять на нашу устойчивость к кибер-угрозам через пять-десять лет. Нам нужны программы «сканирования горизонтов», позволяющие нарабатывать рекомендации по формированию текущей и будущей политики правительства и планированию программ.

Цель

7.4.2. Правительство обеспечит, чтобы программы «сканирования горизонтов» включали в себя тщательную оценку кибер-рисков, и чтобы эта оценка была интегрирована в политику кибербезопасности и развития технологий в других областях наряду с оценкой из других источников и иных доступных фактических материалов. Мы объединим работу по «сканированию горизонтов» в сфере кибербезопасности и в других направлениях политики, чтобы обеспечить целостностный подход к изучению появляющихся вызовов и возможностей.

Наш подход

7.4.3. Мы будем:

- выявлять пробелы в текущей работе и координировать работу в многодисциплинарных рамках, чтобы разработать целостный подход к «сканированию горизонтов» в интересах кибербезопасности;

• содействовать интеграции технических аспектов кибербезопасности с поведенческой наукой;
• поддерживать активный мониторинг рынка криминальных кибер-продуктов для выявления новых инструментов и услуг, которые могут способствовать передаче технологий враждебным государствам, террористам или преступникам;
• анализировать зарождающиеся технологии контроля подключенных к интернету процессов;
• предвосхищать возникновение уязвимостей, связанных с использованием цифровой валюты;
• отслеживать рыночные тенденции в телекоммуникационных технологиях в целях разработки средств ранней защиты от ожидаемых в будущем атак.

7.4.4. Мы признаем, что «сканирование горизонтов» выходит за технические рамки и имеет политическое, экономическое, законодательное, социальное и экологическое измерения. Кибербезопасность — всего лишь один аспект проблем, которые можно разрешить с помощью эффективного «сканирования горизонтов». Поэтому мы обеспечим, чтобы при осуществлении «сканирования горизонтов» в других областях политики учитывались соображения кибербезопасности.

7.4.5. Мы также обеспечим использование подхода, основанного на фактах, к формированию политики кибербезопасности с учетом оценок из всех доступных источников. Они включают в себя, помимо прочего, следующее:

• специфические технические факты, касающиеся, например, «интернета вещей» или будущей роли передовых материалов;
• тенденции развития международных стратегий или общества и их влияние на кибербезопасность.

7.4.6. Мы включим кибербезопасность в сферу компетенции межправительственной группы Government Emerging Technology and Innovation Analysis Cell (ETIAC), которая будет создана с целью обнаружения технологических угроз и определения возможностей, связанных с национальной безопасностью. Кроме того, вопросы кибербезопасности войдут в сферу деятельности уже существующих структур, занимающихся вопросами «сканирования горизонтов», таких как правительственная группа Government Futures Group (GFG) и консультативная группа при секретаре кабинета (Cabinet Secretary’s Advisory Group (CSAG)).

Измерение успеха

7.4.7. Правительство будет измерять успех своей деятельности по внедрению эффективных механизмов «сканирования горизонтов» путем оценки прогресса в достижении следующих результатов:

• межведомственный механизм «сканирования горизонтов» и оценки данных из всех источников интегрирован в процесс формирования политики кибербезопасности;
• соображения кибербезопасности включены во все межведомственные процессы «сканирования горизонтов».

8. МЕЖДУНАРОДНЫЕ ДЕЙСТВИЯ

8.1. Процветание нашей экономики и благосостояние общества все больше зависят от открытости и безопасности сетей, которые выходят за пределы нашего государства. Особое значение приобретает тесное сотрудничество с международными партнерами, направленное на сохранение общего свободного, открытого, мирного и безопасного киберпространства, обеспечивающего эти преимущества. С появлением в мире еще одного миллиарда пользователей интернетом эта задача станет еще важнее.

8.2. Международное сотрудничество в вопросах кибербезопасности стало важной составляющей дебатов по вопросам глобальной экономики и безопасности. Это быстроразвивающаяся область политики, в которой нет единого международного видения. Великобритания и ее союзники добились успеха в установлении некоторых элементов международной системы, основанной на правилах: было достигнуто соглашение о том, что в киберпространстве должно применяться международное право и действовать права человека так же, как и за его пределами; и был достигнут широкий консенсус относительно того, что для решения сложных вопросов, связанных с управлением интернетом, требуется подход, требующий участия всех заинтересованных сторон. Однако с углублением разногласий в отношении того, как решать общую проблему согласования требований национальной безопасности с соблюдением прав и свобод человека, перспективы достижения глобального консенсуса остаются весьма хрупкими.

«Мы должны на международном уровне согласовать «дорожные правила», которые обеспечат будущее процветание и безопасность Великобритании в киберпространстве».

Достопочтенный Борис Джонсон, член парламента, Государственный секретарь

Цели

8.3. Великобритания стремится защитить будущее свободного, открытого и мирного киберпространства в долгосрочной перспективе, содействуя экономическому росту и укреплению национальной безопасности Великобритании. Исходя из этого, Великобритания будет продолжать продвижение модели управления интернетом, предусматривающей участие всех заинтересованных сторон; противостоять локализации данных и содействовать укреплению потенциала наших партнеров по улучшению их кибербезопасности. Для смягчения угроз Великобритании и ее интересам, большая часть которых исходит извне, мы будем искать пути для оказания влияния на принятие решений теми, кто занимается киберпреступностью, кибершпионажем, подрывной и дестабилизирующей деятельностью в киберпространстве, а также продолжим расширять рамки международного сотрудничества.

Наш подход

8.4. В этих целях мы будем:

- укреплять и реализовать на практике общее понимание в отношении ответственного поведения государств в киберпространстве;
- продвигать договоренности о том, что в киберпространстве применяются международные законы;
- продолжать работу по продвижению договоренности о добровольных, необязывающих нормах ответственного поведения со стороны государств;
- оказывать поддержку разработке и внедрению мер укрепления доверия;
- развивать возможности для пресечения деятельности и привлечения к ответственности киберпреступников,

находящихся за рубежом, особенно, в труднодоступных юрисдикциях;
• содействовать созданию условий для сотрудничества наших правоохранительных органов с тем, чтобы в мире оставалось как можно меньше мест, где киберпреступники могут действовать, не опасаясь расследования и привлечения к ответственности;
• способствовать укреплению устойчивости киберпространства за счет формирования технических стандартов, применимых к управлению появляющимися технологиями в международном масштабе (включая шифрование), что поможет автоматически повысить безопасность киберпространства и содействовать применению передовых методик;
• заниматься разработкой общих для государств-единомышленников подходов в отношении возможностей, имеющих трансграничное применение, таких как надежное шифрование;
• содействовать развитию возможностей других стран по противодействию угрозам атаки на Великобританию и ее интересы за рубежом;
• продолжать оказывать содействие нашим партнерам в разработке их стратегий кибербезопасности: у нас общее киберпространство, и уровень коллективной безопасности станет выше, если каждая страна укрепит свою оборону;
• обеспечивать готовность НАТО к конфликтам XXI столетия, которые будут разворачиваться и в киберпространстве, и на поле боя;
• обеспечивать, совместно с нашими союзниками, такую же эффективность операций НАТО в киберпространстве как и на суше, на море и в воздухе;
• обеспечивать, чтобы «Лондонский Процесс», начатый по итогам Глобальной конференции по киберпространству, продолжал содействовать достижению глобального консенсуса в отношении свободного, открытого, мирного и безопасного киберпространства.

8.5. Мы будем продолжать вкладывать средства в развитие отношений и разработку инструментов, содействующих достижению и укреплению всех наших целей в области международной кибербезопасности: достичь этих целей в изоляции невозможно. Среди них:

• установление и сохранение крепких политических и оперативных отношений в тесном взаимодействии с традиционными союзниками и новыми партнерами; создание политических условий, способствующих формированию крепких глобальных альянсов;
• использование нашего влияния в многосторонних организациях, таких как ООН, G20, Европейский Союз, НАТО, ОБСЕ, Совет Европы и Британское Содружество, а также среди развивающихся стран мира;
• укрепление взаимоотношений с организациями негосударственных секторов — бизнеса, гражданского общества, научных кругов и технического сообщества. Они играют важную роль в формировании и критическом анализе международной политики, а также в укреплении политических сигналов по широкому ряду вопросов кибербезопасности. Наши отличные связи с научными кругами могут обеспечить нейтральную платформу для сотрудничества с международными партнерами.

Измерение успеха

8.6. Правительство будет измерять успех своей деятельности по отстаиванию наших международных интересов путем оценки прогресса в достижении следующих результатов:

• благодаря расширению международного сотрудничества были уменьшены угрозы Великобритании и ее зарубежным интересам в киберпространстве;
• достигнуто общее понимание в отношении ответственного поведения государств в киберпространстве;
• международные партнеры повысили свой потенциал кибербезопасности;
• укрепился международный консенсус в отношении преимуществ свободного, открытого, мирного и безопасного киберпространства.

9. МЕТРИКИ

9.1. Отрасль кибербезопасности остается недостаточно сформированной в том, что касается измерения результатов и воздействий — то, что принято называть «метриками». Изучение кибербезопасности уже затруднено из-за использования преувеличений, а также из-за отсутствия выверенных данных. Это вносит элемент отчаяния в работу лиц, отвечающих за формирование политики в организациях и компаниях, которые затрудняются измерить соотношение инвестиций с результатами. Правительство считает, что эффективное использование метрик имеет определяющее значение для реализации этой стратегии и распределения ресурсов, выделяемых на ее реализацию.

9.2. Мы определим всеохватывающий набор строгих метрик для измерения прогресса в достижении необходимых результатов и обеспечим его использование. Создание NCSC, с одной стороны, является одним из основных результатов реализации настоящей стратегии. С другой стороны, он будет играть инструментальную роль в обеспечении возможностей для достижения стратегических результатов в ее рамках другими правительственными ведомствами, предприятиями и обществом.

9.3. В Приложении 3 описывается, каким образом меры измерения успеха, изложенные в настоящей стратегии, будут способствовать достижению стратегических результатов. При этом результаты будут ежегодно пересматриваться, чтобы обеспечить их точное соответствие национальным целям и требованиям. Главные стратегические результаты:

1. Великобритания имеет возможности для эффективного обнаружения, расследования и отражения угроз, связанных с кибероперациями наших противников.

2. Воздействие киберпреступности на Великобританию и ее интересы значительно сократилось, обеспечено сдерживание киберпреступников от атак на цели в Великобритании.

3. Великобритания имеет возможности для управления и эффективного реагирования на кибер-происшествия, уменьшая их пагубные последствия для Великобритании и противодействуя противникам в киберпространстве.

4. Благодаря успешному партнерству с отраслью по созданию активной кибероборонbы большое число фишинговых и вредоносных атак не достигают своей цели.

5. Безопасность Великобритании повысилась в результате того, что в технологических продуктах и услугах настройки кибербезопасности активируются по умолчанию.

6. Правительственные сети и услуги будут защищены на максимальном уровне с момента их развертывания. Население получит возможность пользоваться электронными государственными услугами, будучи уверенным в их безопасности и надежности.

7. Все организации в Великобритании, независимо от размера, эффективно управляют кибер-рисками, опираясь на высококачественные рекомендации NCSC, который обеспечивает их внедрение с помощью сбалансированного сочетания регулятивных требований и стимулов.

8. В Великобритании создана экосистема, необходимая для развития и стабильного функционирования сектора кибербезопасности, способного удовлетворять требования национальной безопасности.

9. В Великобритании создан канал подготовки отечественных кадров, специализирующихся на кибербезопасности, способный удовлетворять растущие потребности экономики, которая становится все более цифровой, как в государственном, так и в частном секторе, а также в области обороны.

10. Великобритания пользуется репутацией общепризнанного мирового лидера по научно-исследовательским разработкам в области кибербезопасности, опирающимся на высокий уровень знаний и опыта в производственной и научной сфере.

11. Британское правительство уже планирует и готовит реализацию политики, предвосхищающей развитие будущих технологий и появление угроз в соответствии с требованиями завтрашнего дня.

12. Сократились угрозы Великобритании и ее зарубежным интересам, благодаря укреплению международного консенсуса и возможностей в отношении ответственного поведения государств в рамках свободного, открытого, мирного и безопасного киберпространства.

13. Упрощены организации, структуры и политика британского правительства с тем, чтобы максимально повысить согласованность и эффективность действий Великобритании в ответ на угрозы в киберпространстве.

9.4. Мы признаем, что некоторые из перспективных планов, предусмотренных настоящей стратегией, выходят за рамки пяти лет ее срока действия. Чтобы будущие инвестиции, вкладываемые в кибербезопасность после 2021 г., продолжали иметь максимально трансформационный эффект, мы намереваемся наметить долгосрочные цели для предприятий, регулирующих органов, аудиторов, страховых компаний и других организаций государственного и частного сектора на период после 2021 года, так как эффективное управление рисками кибербезопасности должно быть интегрировано в стандартную управленческую деятельность каждой организации.

ВЫВОДЫ: КИБЕРБЕЗОПАСНОСТЬ ПОСЛЕ 2021 г.

10.1. Ландшафт киберпространства быстро эволюционирует, и по мере развития технологий постоянно появляются новые проблемы, к использованию которых будут стремиться наши противники. В этой связи настоящая стратегия направлена на то, чтобы дать в наше распоряжение целый ряд правил, инструментов и возможностей, которые помогут нам быстро и гибко реагировать на каждую новую проблему по мере их возникновения.

10.2. Если не принять эффективные меры, угрозы будут эволюционировать быстрее, чем мы сможем подготовиться к защите от них. Мы можем ожидать взрывного роста возможностей для атаки на всех уровнях.

10.3. Если же мы достигнем этих масштабных целей, все ветви британского правительства, бизнес и общество будут принимать участие в обеспечении общегосударственной кибербезопасности. Если мы сможем обеспечить, чтобы параметры безопасности закладывались в массовые технологии на этапе проектирования и активировались по умолчанию, у потребителей и бизнеса будет меньше причин для беспокойства по поводу кибербезопасности. Если Великобритания консолидирует свою репутацию страны, создавшей безопасные условия для ведения бизнеса в сети, сюда придут мировые компании и инвесторы. Повысится безопасность сетей КНИ и приоритетных секторов. Потенциальным противникам, разрабатывающим инструменты и методы атаки на системы, поддерживающие ключевые функции и данные, придется потрудиться, чтобы преодолеть многоуровневую защиту этих систем. Это изменит соотношение риска и вознаграждения для киберпреступников и злоумышленников, которым будет грозить преследование на международном уровне так же, как и за совершение «традиционных» преступлений. Если мы добьемся того, что обеспечение кибербезопасности станет широко распространенной практикой в масштабах всего общества, у Правительства может появиться возможность отказаться от ведущей роли в этом процессе, позволив рынку и технологиям обеспечивать укрепление кибербезопасности в масштабах экономики и общества.

10.4. Даже при самом оптимистичном сценарии для преодоления некоторых сложных или масштабных вызовов, стоящих перед Великобританией в киберпространстве, может потребоваться более пяти лет. В этой связи, настоящая стратегия предоставит в наше распоряжение средства, необходимые для преобразования будущей безопасности и защиты нашего благосостояния в эпоху цифровых технологий.

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ 1: АКРОНИМЫ

CCA — Центр киберoценки. Расположенный в NCSC центр занимается оценкой киберугроз, которую британские правительственные департаменты используют при формировании политики.

CERT — группа реагирования на чрезвычайные происшествия в области компьютерной безопасности.

CERT-UK — группа реагирования на чрезвычайные происшествия в области компьютерной безопасности в Великобритании.

CESG — Национальное техническое управление по информационной безопасности в Великобритании. Предоставляет доступ к надежным и независимым экспертным услугам в области исследований и информационной безопасности, основанным на разведданных, от имени британского правительства

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

> а) значительным пагубным последствиям для доступности, целостности или предоставления наиболее важных услуг, в том числе услуг, нарушение целостности которых может привести к гибели или ранению многих людей, учитывая их серьезные последствия в экономическом и социальном плане;
> и(или)
> б) серьезным последствиям для национальной безопасности, национальной обороны или для функционирования государства.

CPNI — Центр защиты национальной инфраструктуры. Предоставляет рекомендации по сокращению уязвимости организаций, поддерживающих национальную инфраструктуру, к терроризму и шпионажу. Также сотрудничает с NCSC в предоставлении всесторонних рекомендаций по безопасности и защите от угроз в киберпространстве. CPNI поддерживает крепкие партнерские отношения с организациями частного сектора в рамках всей национальной инфраструктуры, создавая надежные условия для взаимовыгодного обмена информацией. В дополнение к прямым взаимоотношениям существует более широкая сеть сотрудничества, включающая другие правительственные департаменты и организации, занимающиеся оказанием профессиональных услуг.

DDoS — распределенная атака типа «отказ в обслуживании». Отправка мощного потока запросов в информационную систему, которые она не в состоянии обработать, в результате чего правомочные пользователи лишаются доступа к ней.

GCHQ — центр правительственной связи, ответственный за ведение радиоэлектронной разведки, при котором работает управление NTA.

ИКТ — информационно-коммуникационные технологии.

MO — Министерство обороны

НАТО — Организация Североатлантического договора.

NCA — Национальное агентство по борьбе с преступностью — правительственный департамент неминистерского уровня.

NCSC — Национальный центр кибербезопасности

ОБСЕ — Организация по безопасности и сотрудничеству в Европе.

МСП — малые и средние предприятия.

ПРИЛОЖЕНИЕ 2: ГЛОССАРИЙ

Action Fraud — Британский национальный центр сбора информации об интернет-преступности, служащий единой точкой контакта для населения и бизнеса.

Активная киберзащита (АКЗ) — принцип реализации мер безопасности, направленных на укрепление защиты сетей или систем с целью повышения их устойчивости к атаками.

Анонимизация — использование инструментальных средств обеспечения анонимности в сети с целью сокрытия личности.

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

Автоматизированная верификация систем — меры обеспечения надлежащей, безошибочной работы программного и аппаратного обеспечения.

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

Большие данные — наборы данных, размер которых достигает такого предела, когда ими становится тяжело оперировать с помощью массового программного обеспечения. Для управления такими объемами данных из большого количества источников и с нужной скоростью требуются особые возможности обработки.

Биткойн — цифровая валюта и платежная система.

Массовое вредоносное программное обеспечение — вредоносные программы, доступные для покупки или бесплатной загрузки, которые не адаптируются для конкретных целей и используются широким спектром злоумышленников.

Computer Network Exploitation (CNE) — кибершпионаж, использование компьютерной сети для проникновения в компьютерную сеть, являющуюся объектом атаки, с целью сбора разведывательной информации.

Рынок киберпреступности — собирательное название продуктов и услуг, поддерживающих экосистему киберпреступности.

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

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

Киберпреступность — кибер-зависимые преступления (преступления, которые можно совершить только с использованием устройств на основе ИКТ и при которых эти устройства являются и орудием, и целью преступления) или преступления, совершаемые с использованием кибер-средств (преступления, которые можно совершить и без использования устройств на основе ИКТ, например финансовое мошенничество, масштаб и охват которых можно существенно увеличить благодаря использованию устройств ИКТ).

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

Кибер-происшествие — инцидент, представляющий или способный 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.

CyberInvest — программа партнерства между отраслью и Правительством, направленная на поддержку самых передовых исследований в области кибербезопасности и защиту Великобритании в киберпространстве, стоимостью 6,5 млн фунтов.

Киберфизическая система — система, подразумевающая интеграцию вычислительных ресурсов и физических процессов; интеллектуальная система.

Устойчивость к киберугрозам — общая способность систем и организаций выдерживать кибератаки и — в случае их успеха — восстанавливаться.

Кибербезопасность — защита взаимосвязанных 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 урон, нанесенный оператором системы умышленно или случайно в результате несоблюдения режима безопасности или под воздействием иных лиц.

Cyber Security Challenge — конкурсы, поощряющие людей проверить свои умения и подумать о карьере в области кибербезопасности.

Киберпространство — взаимосвязанная и взаимозависимая сеть информационных технологических инфраструктур, включая интернет, телекоммуникационные сети, компьютерные системы, взаимосвязанные устройства и встроенные процессоры и контроллеры. Этот термин также может относиться к виртуальному миру или среде, где он обозначает феномен, переживаемый людьми, или абстрактную концепцию.

Кибер-угрозы — все, что может нарушить безопасность или причинить вред информационным системам и взаимосвязанным устройствам (в том числе оборудованию, программному обеспечению и связанной с ними инфраструктуре), данным на них и услугам, которые они предоставляют, преимущественно с использованием киберпространства.

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

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

Система доменных имен (DNS) — система имен компьютеров и сетевых услуг, основанная на доменной иерархии.

Доксинг — получение информации, позволяющей установить личность человека путем поиска в интернете или взлома с последующей ее публикацией.

Электронная коммерция — осуществление экономической деятельности через интернет или при его поддержке.

Шифрование — криптографическое преобразование данных (так называемого «незашифрованного текста») в целях сокрытия их смысла и недопущения их разглашения или использования.

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

Управление происшествиями — организация и координация деятельности по расследованию фактического или потенциального случая враждебной кибератаки, который мог причинить или

причинил ущерб системе или сети, и восстановлению после него.

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

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

Промышленный интернет вещей (ПИВ) — использование технологий интернета вещей в производстве и промышленности.

Инсайдер — лицо, имеющее доверенный доступ к данным и информационным системам организации и представляющее риск умышленной, случайной или неосознанной киберугрозы.

Целостность — свойство информации, означающее, что она не была случайно или умышленно изменена и является точной и полной.

Интернет — всемирная компьютерная сеть, включающая разнообразные информационно-коммуникационные объекты, состоящие из взаимосвязанных сетей, пользующихся стандартизированными протоколами передачи данных.

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

Лондонский процесс — комплекс мер, определенный по итогам Лондонской конференции по киберпространству 2011 г.

Вредоносное программное обеспечение — вредоносные программы или коды. К вредоносному программному обеспечению относятся вирусы, черви, трояны и шпионское ПО.

Сеть (компьютерная) — система, объединяющая узловые компьютеры с подсетевыми или межсетевыми устройствами, через которые осуществляется обмен данными между ними.

Наступательные кибероперации — использование кибернетических возможностей с целью вывода из строя, блокирования, ухудшения работы или уничтожения, компьютеров, сетей и взаимосвязанных устройств.

Исправление уязвимостей — процесс обновления программного обеспечения с целью устранения ошибок и уязвимостей.

Тестирование на проникновение — метод оценки устойчивости сети или объекта ко взлому, санкционированный или спонсированный тестирующей организацией.

Фишинг — использование электронной почты для рассылки писем, составленных таким образом, чтобы быть максимально похожими на настоящие письма от надежного источника с целью обманным путем заставить получателя перейти по ссылке на вредоносный сайт, открыть приложение, зараженное вредоносным ПО, или передать секретную информацию неизвестной третьей стороне.

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

Рекогносцировка — этап атаки, на котором злоумышленник собирает информацию о сетях или подключается к ним, а также

проводит разведку на наличие уязвимостей с целью взлома.

Риск — возможная опасность того, что в результате атаки могут быть использованы уязвимости информационной системы для причинения вреда.

Маршрутизатор — устройство, связывающее логические сети путем пересылки информации в другие сети на основе IP-адресов.

«Скрипт-кидди» — дилетант, использующий готовые скрипты или программы, которые можно найти в интернете, для осуществления атак, таких как дефейс веб-сайта.

Безопасность по умолчанию — настройки безопасного пользования технологиями массового потребления, которые устанавливаются для пользователей по умолчанию.

Интегрированная в дизайн безопасность — программное обеспечение, оборудование и системы, которые изначально проектировались из расчета на безопасность.

SMS-спуфинг — прием маскировки адреса отправителя SMS-сообщения путем замены оригинального номера мобильного телефона (идентификатора отправителя) буквенно-цифровым текстом. Может законно использоваться отправителем, например, для замены собственного номера телефона на свое имя или название компании. Или незаконно, например, для того чтобы выдать себя за другое лицо в мошеннических целях.

Социальная инженерия — методика, используемая злоумышленниками для того, чтобы обманным путем заставить жертву выполнить какое-либо действие или раскрыть конфиденциальную информацию. Как правило, от жертвы требуется, чтобы она перешла на вредоносный сайт или открыла ненужное ей файловое приложение.

Trusted Platform Module (TPM) — международная спецификация, описывающая криптопроцессор, в котором хранятся криптографические ключи для защиты аппаратного обеспечения.

Пользователь — лицо, организация или автоматизированный процесс, получающий авторизованный или не авторизованный доступ к системе.

Вирусы — вредоносные компьютерные программы, способные заражать другие файлы.

Вишинг или «голосовой фишинг» — использование голосовых технологий (аналоговых телефонов, мобильных телефонов, голосовых сообщений и т. д.) для того, чтобы заставить человека раскрыть секретную финансовую или персональную информацию неавторизованным лицам, как правило, в мошеннических целях.

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

ПРИЛОЖЕНИЕ 3: ПРОГРАММА ДОСТИЖЕНИЯ КЛЮЧЕВЫХ ПОКАЗАТЕЛЕЙ

НАЦИОНАЛЬНАЯ СТРАТЕГИЯ КИБЕРБЕЗОПАСНОСТИ 2016-2021

Видение: в Великобритании обеспечены безопасность, устойчивость к киберугрозам, процветание и условия для уверенного пользования цифровыми технологиями.

Стратегические результаты	Индикативные меры успеха (до 2021 г.)	Направление
1. Великобритания имеет возможности для эффективного обнаружения, расследования и отражения угроз, связанных с кибероперациями наших противников.	• Укрепление сетей, учрежденных нами для обмена информацией с международными партнерами, и расширение многосторонних соглашений, утверждающих законное и ответственное поведение со стороны государств, помогают нам лучше понять угрозы, реагировать на них и в конечном итоге укрепить оборону Великобритании. • В результате принятия мер по укреплению обороны и сдерживанию, наряду со стратегиями по отдельным странам, созданы условия, в которых враждебным иностранным субъектам и кибертеррористам становится трудно обеспечивать успех атак на Великобританию. • Улучшено понимание киберугрозы со стороны враждебных иностранных субъектов и террористов, путем определения и расследования угроз террористических атак на Великобританию. • Предотвращено наращивание возможностей для кибер-террористической деятельности в долгосрочной перспективе с помощью мониторинга, а также разрушения потенциала и пресечения кибер-террористической деятельности при первой возможности. • Великобритания является одним из мировых лидеров по возможностям для наступательных кибероперациий. • Великобритания создала канал подготовки квалифицированных кадров, необходимых для разработки и развертывания суверенных наступательных возможностей в киберпространстве. • Наши суверенные криптографические возможности являются эффективными в контексте защиты тайн и секретной информации от несанкционированного раскрытия.	СДЕРЖИВАНИЕ
2. Воздействие киберпреступности на Великобританию и ее интересы значительно сократилось, обеспечено сдерживание киберпреступников от атак	• Повысилась результативность деятельности по пресечению кибер-атак на Великобритании, в том числе увеличилось число арестов и обвинительных приговоров и было уничтожено больше криминальных сетей в результате действий правоохранительных органов;	СДЕРЖИВАНИЕ

на цели в Великобритании.	• Улучшены возможности правоохранительных органов, в том числе: расширен потенциал и повысился уровень квалификаций специалистов и персонала в общем, а также расширены правоохранительные возможности наших зарубежных партнеров. • Повысилась эффективность и масштабность мер раннего воздействия по отвращению от криминальной деятельности и перевоспитанию правонарушителей; • В результате того, что затруднился доступ к криминальным кибер-услугам и снизилась их эффективность, сократилось число киберпреступлений низкого уровня.	
3. Великобритания имеет возможности для управления и эффективного реагирования на кибер-происшествия, уменьшая их пагубные последствия для Великобритании и противодействуя противникам в киберпространстве.	• Увеличивается доля происшествий, о которых пострадавшие сообщают в органы власти, что позволяет лучше понять размер и масштаб угрозы. • В результате создания Национального центра кибербезопасности в качестве централизованного механизма сбора информации об угрозах и реагирования на атаки осуществляется более эффективное и комплексное управление киберугрозами. • Мы будем работать над искоренением основных причин атак на национальном уровне, сокращая число случаев повторного использования уязвимостей в системах различных пользователей и секторов.	ОБОРОНА
4. Благодаря успешному партнерству с отраслью в области создания активной кибероборонымасштабные фишинговые и вредоносные атаки не достигают своей цели.	• В Великобритании стало сложнее осуществлять фишинговую деятельность, так как мы обеспечили масштабную защиту от использования вредоносных доменов, внедрили более активную и масштабную защиту от фишинга, равно как и других форм коммуникаций в рамках атак социальной инженерии, например, «вишинга» и SMS-спуфинга. • Блокируется гораздо больше вредоносных коммуникаций и технических артефактов, связанных с кибератаками и использованием уязвимостей. • Британский интернет- и телекоммуникационный трафик значительно менее уязвим к попыткам перемаршрутизации со стороны злонамеренных субъектов. • Значительно расширились возможности GCHQ, вооруженных сил и NCA по реагированию на серьезные угрозы со стороны субъектов, спонсируемых государством, и преступников.	ОБОРОНА
5. Безопасность Великобритании повысилась в результате	• Большая часть продуктов потребления и услуг, доступных в Великобритании в 2021 г., способствует максимальному повышению	ОБОРОНА

того, что в технологических продуктах и услугах настройки кибербезопасности активируются по умолчанию.	безопасности Великобритании, благодаря автоматической активации в них встроенных настроек «безопасности по умолчанию» или обеспечению безопасности на этапе проектирования. • Население Великобритании уверенно пользуется государственными услугами, поскольку они максимально защищены, а уровни вероятного мошенничества находятся в пределах приемлемых параметров риска.	
6. Правительственные сети и услуги будут защищены на максимальном уровне с момента их развертывания. Население получит возможность пользоваться электронными государственными услугами, будучи уверенным в их безопасности и надежности.	• Правительство имеет глубокое понимание уровней риска кибербезопасности в масштабах всего правительства и государственного сектора в целом. • Отдельные правительственные учреждения и другие органы обеспечивают защиту, пропорциональную уровню риска и в соответствии с согласованными минимальными государственными стандартами. • Правительственные департаменты и другие государственные органы устойчивы к угрозам и способны эффективно реагировать на кибер-происшествия, сохраняя функциональность и обеспечивая быстрое восстановление. • Новые технологии и цифровые сервисы, развертываемые правительством будут иметь настройки «кибербезопасности по умолчанию». • Мы осведомлены обо всех известных уязвимостях правительственных систем и служб, имеющих выход в интернет, и активно их устраняем. • Все поставщики правительства обеспечивают соответствие необходимым стандартам кибербезопасности.	ОБОРОНА
7. Все организации в Великобритании, независимо от размера, эффективно управляют кибер-рисками, опираясь на высококачественные рекомендации NCSC, который обеспечивает их внедрение, с помощью сбалансированного сочетания регулятивных требований и стимулов.	• Мы понимаем уровень кибербезопасности в масштабах всей КНИ и предусмотрели необходимые меры вмешательства, чтобы в случае необходимости обеспечить улучшение ситуации в национальных интересах. • Самые важные компании и организации понимают существующий уровень угроз и в соответствии с ним внедряют правила кибербезопасности. • Уровень безопасности британской экономики сопоставим с уровнем кибербезопасности в развитых странах или превышает его. • Количество, серьезность и последствия успешных кибератак на компании в Великобритании сократились в результате улучшения и соблюдения элементарных правил.	ОБОРОНА

	• Культура кибербезопасности улучшилась в масштабах всей Великобритании в результате того, что организации и население понимают существующие кибер-риски и знают, что необходимо делать для управления ими.	
8. В Великобритании создана экосистема, необходимая для развития и стабильного функционирования сектора кибербезопасности, способного удовлетворять требования национальной безопасности.	• Достигнутые темпы ежегодного роста британского кибер-сектора превышают среднемировые. • Существенно увеличился объем инвестиций в молодые компании.	РАЗВИТИЕ
9. В Великобритании создан канал подготовки отечественных кадров, специализирующихся на кибербезопасности, способный удовлетворить растущие потребности цифровой экономики, как в государственном, так и в частном секторе, а также в области обороны.	• Существуют действенные и четко обозначенные пути выбора профессии специалиста по кибербезопасности, привлекательные для широкого круга людей. • К 2021 г. кибербезопасность практически стала неотъемлемой составляющей соответствующих учебных программ на всех уровнях системы образования — от начальной школы до последипломного обучения. • Профессия специалиста по кибербезопасности утвердилась, получила широкое признание и Королевский Диплом, оформились пути карьерного роста. • Изучение кибербезопасности в определенном объеме вошло в программы повышения квалификации соответствующих работников, не специализирующихся на кибербезопасности, в масштабах всей экономики. • Правительство и Вооруженные силы имеют доступ к специалистам по кибербезопасности, способным поддерживать безопасность и устойчивость Великобритании к угрозам.	РАЗВИТИЕ
10. Великобритания пользуется репутацией общепризнанного мирового лидера по научно-исследовательским разработкам в области кибербезопасности, опирающимся на высокий уровень знаний и опыта в производственной и научной сфере.	• Существенно увеличилось число британских компаний, достигших успеха в выводе в коммерческое обращение плодов научных исследований в области кибербезопасности. За счет эффективного восполнения недостатков в возможностях по обеспечению кибербезопасности их стало меньше. • Великобритания пользуется репутацией мирового лидера по исследованиям и инновациям в области кибербезопасности.	РАЗВИТИЕ
11. Британское правительство уже	• Межведомственный механизм «сканирования горизонтов» и оценки	РАЗВИТИЕ

планирует и готовит реализацию политики, предвосхищающей развитие будущих технологий и появление угроз в соответствии с требованиями завтрашнего дня.	данных из всех источников интегрирован в процесс формирования политики кибербезопасности. • Соображения кибербезопасности включены во все межведомственные процессы «сканирования горизонтов».	
12. Сократились угрозы Великобритании и ее зарубежным интересам, благодаря укреплению международного консенсуса и возможностей в отношении ответственного поведения государств в рамках свободного, открытого, мирного и безопасного киберпространства.	• Благодаря расширению международного сотрудничества были уменьшены угрозы Великобритании и ее зарубежным интересам в киберпространстве. • Достигнуто общее понимание в отношении ответственного поведения государств в киберпространстве. • Международные партнеры повысили свой потенциал кибербезопасности. • Укрепился международный консенсус в отношении преимуществ свободного, открытого, мирного и безопасного киберпространства.	МЕЖДУНАРОДНАЯ ДЕЯТЕЛЬНОСТЬ И ВЛИЯНИЕ
13. Упрощены организации, структуры и политика британского правительства с тем, чтобы максимально повысить согласованность и эффективность действий Великобритании в ответ на угрозы в киберпространстве.	• Существует понимание обязанностей Правительства в области кибербезопасности, а его услуги являются доступными. • Наши партнеры знают, как лучше всего взаимодействовать с Правительством по вопросам кибербезопасности.	ПО ВСЕМ НАПРАВЛЕНИЯМ