Секция «Международная безопасность: новые вызовы и угрозы»

Кибербезопасность Великобритании: новые вызовы, новые решения

Научный руководитель – Кулькова Ольга Сергеевна

Климова Анастасия Сергеевна

Аспирант

Московский государственный университет имени М.В.Ломоносова, Факультет мировой политики, Кафедра международной безопасности, Москва, Россия

E-mail: mudrie1@mail.ru

Обеспечение кибербезопасности очень важно для правительства Великобритании на современном этапе. С каждым годом в этой сфере появляются новые угрозы и вызовы, борьба с которыми подчас требует не только новых технологических решений, но и новых политических усилий.

Безопасная онлайн-среда имеет критическое значение для Великобритании как одной из лидирующих цифровых экономик в мире. К 2020 г., по данным ежегодного отчета о реализации Стратегии Великобритании по кибербезопасности за 2016 г., количество устройств, подключенных к "интернету вещей", возрастет в мире до 20 миллиардов [1]. Это качественный и количественный рывок вперед по сравнению с началом 2000-х гг., порождающий новый масштаб вызовов.

С 2011 по 2016 гг. объемы цифровой экономики Великобритании выросли с 10 до 17 млрд. фт. ст., в ней на данный момент занято около ста тысяч сотрудников. В Великобритании на настоящем этапе в день регистрируется более 600 попыток взломать сайты и базы данных различных государственных структур, в том числе налоговой службы и министерства иностранных дел [2]. При этом только в 2010 г. экономика страны понесла ущерб в размере 27 млрд. фунтов в результате компьютерных преступлений, в том числе мошенничества с кредитными картами и похищения интеллектуальной собственности [3]. Эти факты свидетельствуют о том, что проблема компьютерной безопасности является предельно острой и имеет непосредственное отношение к вопросам экономической стабильности и обороноспособности страны.

Актуальность и значимость киберугроз, стоящих перед страной, нашла свое отражение в стратегиях национальной безопасности 2010 и 2015 гг, принятых во время премьерства Д. Кэмерона. В Стратегии 2010 г. киберугрозы были обозначены в качестве приоритетов высочайшей важности (Tier 1). В Стратегии 2015 г. Великобритания признана мировым лидером в обеспечении кибербезопасности, при партнерстве государства, бизнеса и науки в сфере кибербезопасности. Однако число киберугроз не только не идет на убыль, а возрастает.

Именно поэтому обеспечение кибербезопасности стало приоритетом политики Великобритании в области национальной безопасности.

Особый акцент правительство Великобритании делает на борьбе с кибертерроризмом и кибершпионажем. Кибертерроризм подразумевает использование сети Интернет для преднамеренного крупномасштабного разрушения компьютерных сетей посредством компьютерных вирусов, фишинга и других вредоносных программ и аппаратных методов и сценариев программирования. Враждебные акторы, осуществляющие кибершпионаж, нарушают работу правительства и могут также использовать вредоносное ПО для разрушения и повреждения киберинфраструктуры.

В 2010-2016 гг. в Великобритании были приняты конкретные и важные меры по борьбе с кибертерроризмом. В 2011 г. траты страны на обеспечение информационной безопасности (включая прямые потери, восстановление данных, поддержание безопасности и т.д.)

составляли около 32 млрд фунтов [4]. В настоящее время киберпреступность является самым распространенным видом преступлений в Великобритании. Бизнес-сектор Великобритании понес убытки в объеме 1 миллиарда фунтов стерлингов из-за онлайн-преступлений в 2015-2016 гг. [9].

Государство оказывает поддержку развивающейся в Великобритании отрасли кибербезопасности, идет подготовка первоклассных специалистов в данной области. Обеспечение кибербезопасности в Великобритании является быстрорастущей отраслью, где заняты порядка 58 тысяч специалистов [5]. Финансирование деятельности по обеспечению кибербезопасности в новой Стратегии национальной безопасности Великобритании 2015 г. было увеличено практически в два раза по сравнению с первой стратегией 2010 г. Были существенно увеличены инвестиции правительства в защиту Великобритании от кибератак и развития киберпространства (до 1,9 млрд. фунтов стерлингов) [6]. 1 ноября 2016 г. канцлер казначейства Великобритании Филип Хэммонд официально представил новую национальную Стратегию правительства по кибербезопасности. Согласно данным стратегии, в течение 2016-2021 гг. будет вложено в общей сложности 2,9 млрд фунтов в кардинальную трансформацию системы кибербезопасности Великобритании [7].

По сравнению с 2011 г., изменился стратегический контекст, произошли значительные технические изменения, поменялся и геополитический ландшафт. Главными киберугрозами в новой стратегии названы кибермошенничество, кражи и вымогательства в интернете. Для борьбы с указанными угрозами разработан ряд мер: увеличение инвестиций в кибербезопасность, запуск двух центров киберинноваций, усиление вооруженных сил в плане реагирования на киберугрозы, минимизирование количества атак с подозрительных IP-адресов.

Киберпространство предоставляет значительную возможность для экономического роста и социального развития. Несмотря на то, что интернет рассматривается правительством Великобритании как платформа для инноваций и новых источников роста, он представляет ряд угроз для экономики государства. Постоянное появление новых видов киберугроз требует своевременного ответа и новых методов отражения кибератак.

Озабоченность по поводу киберугроз в странах ЕС и в Великобритании нарастает. Лидеры международного бизнеса и правительственные чиновники на Мюнхенской конференции по безопасности в 2018 г. указали на кибертерроризм как на главную угрозу международной безопасности [8].

Источники и литература

1) The UK Cyber Security Strategy 2011-2016 Annual Report. Cabinet Office. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf
2) Cybercrime and fraud scale revealed in annual figures. 19 January 2017. BBC. URL: http://www.bbc.com/news/uk-38675683
3) Национальная стратегия кибербезопасности Великобритании 2011 г. UK National cybersecurity strategy 2011.
4) Total Public Spending in the United Kingdom Central Government and Local Authority. UK Public Spending Data. URL: https://www.ukpublicspending.co.uk
5) Вискалин, В. В школах Великобритании введут уроки по кибербезопасности. 11 февраля 2017 г. Rusbase. https://rb.ru/news/cyber-urok/
6) Britain's cyber security bolstered by world-class strategy. News story. 1 Novemner 2016. HM Govermment. URL: https://www.gov.uk/government/news/britains-cyber-security-bolstered-by-world-class-strategy

7) Национальная стратегия кибербезопасности Великобритании 2016-2021 гг. HM Government, 2016. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/643426/Russian_translation_-_National_Cyber_Security_Strategy_2016.pdf

8) Amaro, S. and Gamble, H. Cyberattacks are the single greatest threat to global stability, German defense minister says. 17 Feb 2018. CNBC. URL: https://www.cnbc.com/2018/02/17/munich-security-conference-german-defense-minister-on-global-stability.html

9) Over £1bn lost by businesses to online crime in a year. 13th june 2016. Action Fraud. National Fraud & Cyber Crime Reporting Centre. URL: https://www.actionfraud.police.uk/news/over-1bn-lost-by-businesses-to-online-crime-in-a-year-jun16