УДК 355.01:621.391

Вавринюк Сергей Адамович

старший преподаватель
Военная академия связи им. Маршала
Советского Союза С.М. Буденного
Санкт-Петербург, Россия

Sergey A. Vavrinyuk

senior lecturer
Military Academy of Communications named after
Marshal of the Soviet Union S.M. Budyonny
St. Petersburg, Russia

Иванов Андрей Анатольевич

профессор, кандидат технических наук, доцент
Военная академия связи им. Маршала
Советского Союза С.М. Буденного
Санкт-Петербург, Россия

Andrey A. Ivanov

Professor, Candidate of Technical
Sciences, Associate Professor
Military Academy of Communications named after
Marshal of the Soviet Union S.M. Budyonny
St. Petersburg, Russia

Яковицкий Сергей Анатольевич

профессор, кандидат военных наук, доцент
Военная академия связи им. Маршала
Советского Союза С.М. Буденного
Санкт-Петербург, Россия
logoshik@mail.ru

Sergey A. Yakovitsky

senior lecturer
Military Academy of Communications named after
Marshal of the Soviet Union S.M. Budyonny
St. Petersburg, Russia

ОСНОВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ КОНТРРАЗВЕДКИ США НА БЛИЖАЙШИЕ ГОДЫ

MAIN DIRECTIONS OF DEVELOPMENT OF US COUNTERINTELLIGENCE IN THE COMING YEARS

Аннотация

Высшее военно-политическое руководство США уделяет большое внимание актуализации руководящих документов национального уровня в области обороны и безопасности. Обновленная в августе 2024 года Национальная стратегия контрразведки США представляет собой комплексный подход к противодействию иностранным разведывательным угрозам. Эффективная реализация этой стратегии требует координации усилий на всех уровнях правительства, а также активного взаимодействия с частным сектором, академическими кругами, международными партнерами и информированной общественности.

Abstract

The top military and political leadership of the United States pays great attention to updating national-level guidance documents in the field of defense and security. Updated in August 2024, the US National Counterintelligence Strategy represents a comprehensive approach to countering foreign intelligence threats. Effective implementation of this strategy requires coordination of efforts at all levels of Government, as well as active interaction with the private sector, academia, international partners and an informed public.

Ключевые слова:

вооруженные силы, иностранная разведка, национальная безопасность, разведывательное сообщество

Keywords:

Armed Forces, foreign intelligence, national security, intelligence community

Высшее военно-политическое руководство США уделяет большое внимание совершенствованию системы контрразведки государства в целях обеспечения национальной безопасности США.

Рис.1 Эмблема национального центра контразведки и безопасности

В целом за организацию и ведение контрразведки в США отвечает Национальный центр контрразведки и безопасности (НЦКБ) (National Counterintelligence and Security Center - NCSC), входящий в состав Управления Национальной разведки (рис. 1). Возглавляет НЦКБ – директор Национальной контрразведки, который подчиняется Директору Национальной разведки США.

В США контрразведкой занимаются:

1) Центральное разведывательное управление (ЦРУ) - основной орган внешней разведки и контрразведки. Он не имеет функций правоохранительных органов и в основном сосредоточен на внешней разведке, но с некоторыми элементами внутренней разведки и контрразведки;

2) Федеральное бюро расследований (ФБР) - федеральное правоохранительное агентство и орган внутренней разведки и контрразведки, орган антитеррористической деятельности;

3) в Министерстве внутренней безопасности: Агентство по кибербезопасности и безопасности инфраструктуры США;

4) в Министерстве обороны: Агентство национальной безопасности (АНБ), Объединенное кибернетическое командование, Командования разведки и безопасности видов Вооруженных сил (ВС), части и подразделения контрразведки ВС;

5) другие структуры, входящие в Разведывательное сообщество США.

В последнее время ряд министерств и ведомств США создают свои структуры для решения задач противостояния разведкам и шпионажу. Так, в 2023 году Министерство торговли создало новое управление, которое будет решать вопросы комплексного анализа торговой/коммерческой деятельности, заключаемых договоров и будет придерживаться стандартов Разведсообщества.


Department of Defense
INSTRUCTION

Рис.2. Инструкция министра оборонь США «Противодействие шпионажу, международному терроризму и контрразведке» (2020 г.)

Несмотря на то, что контрразведка включает в себя обеспечение безопасности, в ее основе лежит анализ. Она действует как основополагающий процесс, который объединяет различные формы разведывательной работы.

В Вооруженных силах США контрразведка организована в соответствии руководящими документами министерства обороны, разработанными в свою очередь на основе действующей Национальной стратегии контрразведки (National Counterintelligence Strategy) (рис. 2).

Применительно к Сухопутным войскам США, если ранее вопросы организации и ведения контрразведки рассматривались в полевом уставе FM 2-22.2 (2009 года), то в последующем они были перемещены в документы ограниченного доступа и лишь небольшие упоминания, о целях и задачах контрразведки имеются в наставлении ADRP 2-0 (2012 г.) и полевом уставе FM 2-0 (2023 г.) (рис. 3).

Рис.3 Руководящие документы Сухопутных войск США по организации контрразведки, находящиеся в открытом доступе: полевой устав FM 2-22.2 «Контрразведка» (2009 г.), наставление ADRP 2-0 «Разведка» (2012), полевой устав FM 2-0 (2023 г.)

Контрразведка США отвечает за:

1) выявление и нейтрализацию деятельности иностранных разведок;

2) защиту от внутренних угроз;

3) защиту конфиденциальной и секретной информации;

4) защиту критически важных объектов от технических проникновений, шпионажа и других угроз разведки;

5) защиту интересов, активов и граждан США (иногда и «важных» иностранных персон) внутри страны и за рубежом от саботажа, покушений, причинения вреда здоровью, убийств или других действий и операций иностранных разведок.

Высшее военно-политическое руководство США уделяет большое внимание актуализации руководящих документов национального уровня в области обороны и безопасности [1]. Согласно принятому в 2002 году в США закону об усилении контрразведки Национальная Стратегия контрразведки должна утверждаться раз в четыре года.

В этой связи 01.08.2024 г. президентом США была утверждена обновленная Национальная стратегия контрразведки США 2024 (далее – Стратегия) (рис. 4). Предыдущие были приняты в 2016 и 2020 годах.

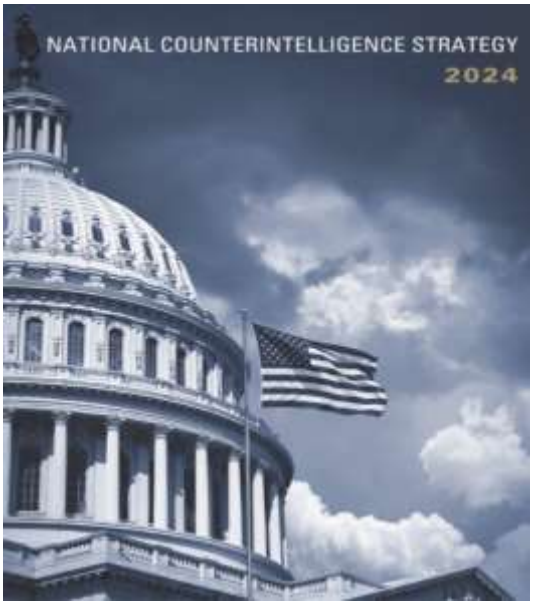

Рис.4 Национальная стратегия контрразведки США (2024 г.)

Документ включает в себя секретную часть и вариант для открытой публикации.

Обновленная Стратегия разработана Национальным центром контрразведки и безопасности совместно с администрацией Белого Дома и Разведывательным сообществом. Она определяет основу для стратегической контрразведывательной программы действий различных государственных структур и организаций США для выявления и пресечения деятельности иностранных разведок как внутри страны, так и за рубежом. Пересмотрены приоритеты ведения контрразведки для решения как текущих, так и прогнозируемых угроз.

Новая Стратегия выделяет три важнейших направления деятельности контрразведки США на ближайшие три года:

1) Противодействие иностранным разведывательным структурам и сдерживание их действий;

2) Защита стратегических преимуществ США;

3) Инвестирование в будущее.

В документе отмечается, что США сейчас сталкиваются с беспрецедентными по своей широте, объему, сложности и влиянию угрозами со стороны иностранных разведывательных служб. Данные структуры активно используют современные технологии: новейшие системы связи, передачи и распределения данных, системы анализа и обработки информации, кибернетические инструменты, коммерческое шпионское программное обеспечение, биометрические устройства, беспилотные системы, изображения высокого разрешения, усовершенствованное техническое оборудование для наблюдения, искусственный интеллект и другие. Эти инструменты относительно просты в использовании, сравнительно дешевы и доступны в коммерческом плане, что делает их привлекательными даже для небольших разведывательных органов и организаций. Экспоненциальный темп технологических изменений усложняет усилия по разработке и поддержанию адекватной защиты. Все это представляют собой непосредственную угрозу национальной, экономической безопасности США, демократическим процессам и общественной сплоченности [2].

Россия и Китай рассматриваются как основные источники угроз для США. Особое опасение США вызывает расширение взаимного сотрудничества этих стран во многих сферах, в первую очередь в военной. Угрозу также представляют Иран, КНДР, а также множественные частные негосударственные разведывательные структуры.

Для достижения поставленных целей по первому направлению деятельности контрразведки США (противодействие иностранным разведывательным структурам и сдерживание их действий) необходимо решение следующих задач:

1. Обнаружение, понимание и прогнозирование угроз иностранной разведки.

Для решения данной задачи правительство США планирует:

- расширение возможностей по сбору и анализу информации о планах, намерениях и уязвимостях иностранных разведывательных служб;

- улучшение механизмов обмена информацией между федеральными, государственными и местными органами, частным сектором и иностранными партнерами;

- усиление стандартов и процессов сбора, анализа и обработки информации для повышения качества контрразведывательной деятельности.

Противодействие, ухудшение и сдерживание деятельности и возможностей иностранной разведки.

Для этого необходимо:

- использование полного спектра контрразведывательных полномочий и инновационных инструментов для выявления и нейтрализации угроз;

- выявление и нейтрализацию нетрадиционных способов и средств ведения разведки;

- увеличение интеграции и координации стратегических контрразведывательных мероприятий для формирования информационной среды и сдерживания угроз.

Борьба с кибердеятельностью иностранной разведки.

Пути решения:

- развитие партнерских отношений между федеральными, государственными и местными органами власти, частным сектором, академическими кругами и с зарубежными партнерами для обмена информацией, повышения прозрачности и укрепления доверия для получения информации для выявления и нейтрализации киберугроз;

- внедрение инновационных решений для повышения стоимости и риска кибердеятельности иностранных разведывательных служб.

Для достижения поставленных целей по второму направлению деятельности контрразведки США (защита стратегических преимуществ США) необходимо решение следующих задач:

Защита граждан от преследований и сбора данных иностранными разведками.

Пути решения:

- выявление угроз и обнаружение действий иностранных разведок в отношении отдельных лиц;

- повышение оперативности и достоверности получаемой разведывательной информации;

- расширение взаимодействия с государственными, местными органами управления, иностранными правительствами, партнерами из частного сектора и

общественностью США для информирования о принятии решений, расширении прав и возможностей целевых лиц и повышения риска для операций иностранных разведок.

Защита демократии от иностранного злонамеренного влияния.

Пути решения:

- расширение знаний граждан о возможностях иностранных разведок, методов и приоритетов их действий по всему спектру возможных субъектов;

- расширение взаимодействия и создание прочных партнерских отношений между федеральными, государственными, местными органами власти, иностранными правительствами, а также с частным сектором, гражданским обществом и академическими кругами для обмена информацией и знаниями, повышения осведомленности об угрозах злонамеренного влияния иностранных разведок, обеспечения действий и укрепления доверия и устойчивости;

- разработка индивидуальных инструментов и процессов для улучшения обмена информацией, прозрачности и сотрудничества для поддержки более быстрых, скоординированных действий по выявлению и пресечению действий иностранных разведок.

Защита критически важных технологий и экономической безопасности США.

Китай рассматривается как страна, вызывающая наибольшую озабоченность в этой сфере, поскольку она нацелена на ключевые технологические секторы и конфиденциальные коммерческие и военные технологии США, союзных стран и научно-исследовательских институтов и использует различные инструменты, включая шпионаж и кражу, для развития своих технологических возможностей.

Пути решения:

- усиление аналитических возможностей и улучшение процессов выявления угроз для критических технологий и данных;

- укрепление партнерств с частным сектором и академическими кругами для повышения осведомленности и противодействия угрозам, информирования и обеспечения мероприятий по смягчению угроз.

4. Защита критической инфраструктуры страны.

По докладам руководства ФБР, АНБ и Агентства кибербезопасности и инфраструктурной безопасности США киберативность Китая выходит за рамки шпионажа и кражи данных последнего десятилетия и переходит к прямым атакам на критически важную инфраструктуру США. Так, в 2023 году был вскрыт факт внедрения

вредоносного программного обеспечения китайской хакерской группой «Волт Тайфун» (Volt Typhoon) на сетевые маршрутизаторы и другие устройства, подключенные к Интернету, которое в случае срабатывания может нарушить водоснабжение, электроснабжение и транспортные системы, функционирование нефте- и газопроводов, причинить реальный вред американским гражданам и сообществам. По оценкам экспертов, Китай готовит «цифровой ландшафт» к возможной военной активности, что является огромным скачком от простого шпионажа и кражи данных [3].

В тоже время основные направления кибердеятельности России – политическое воздействие (оказание влияния на выборы, политические кампании) в США и нарушение критически важных систем Украины.

Пути решения:

- развитие партнерства с частным сектором, федеральными, государственными, местными, органами, а также другими структурами для улучшения координации и сотрудничества, укрепления доверия и обеспечения действий;

- внедрение инновационных аналитических инструментов для выявления и прогнозирования угроз.

5. Снижение рисков для ключевых цепочек поставок.

Пути решения:

- улучшение аналитических методов и углубление интеграции существующих усилий по управлению рисками цепочек поставок;

- увеличение взаимодействия с партнерами для обмена информацией, укрепления доверия и получения информации о текущих уязвимостях цепочки поставок и будущих областях инвестиций для лучшего понимания, предвидения и смягчения угроз;

- совершенствование системы сбора информации о планах, намерениях, доступе и возможностях иностранных разведок для использования, нарушения или саботажа ключевых цепочек поставок.

Для достижения поставленных целей по третьему направлению деятельности контрразведки США (инвестирование в будущее) необходимо решение задачи:

Развитие возможностей контрразведки, партнерств и устойчивости.

Пути решения:

- инвестирование в инновационные технологии и интегрированные решения;

- набор, обучение и удержание квалифицированных кадров с необходимыми знаниями, навыками и специализированным опытом для реагирования на текущие и будущие угрозы;

- укрепление партнерских отношений и сотрудничества для повышения осведомленности, обмена информацией и устойчивости к угрозам.

Таким образом, высшее военно-политическое руководство США полагает, что интересы национальной и экономической безопасности США будут по-прежнему сталкиваться с серьезными угрозами со стороны внешней разведки. Обновленная Национальная стратегия контрразведки США представляет собой комплексный подход к противодействию иностранным разведывательным угрозам. Эффективная реализация этой стратегии требует координации усилий на всех уровнях правительства, а также активного взаимодействия с частным сектором, академическими кругами, международными партнерами и информированной общественности.

Список использованных источников

1. Яковицкий С.А., Иванов А.А., Вавринюк С.А. Система руководящих документов США в области обороны. Научный аспект. 2024. Т. 15. № 3. С. 1750-1757.

2. National counterintelligence strategy [сайт]. – URL: https://www.dni.gov/files/NCSC/documents/features/NCSC_CI_Strategy-pages-20240730.pdf./(Дата обращения 02.08.2024). – Текст : электронный.

3. Chinese hacking operations have entered a far more dangerous phase, US warns [сайт]. – URL: https://www.defenseone.com/technology/2024/02/chinese-hacking-operations-have-entered-far-more-dangerous-phase-us-warns/393843/ Patrick Tucker. (Дата обращения 02.08.2024). – Текст : электронный.