DOI 10.22394/2073-2929-2020-1-94-102

Проблемы обеспечения кибербезопасности России в Арктике

Лукин Ю. Ф.
Высшая школа Российской Федерации, Академия геополитических проблем, Архангельск, Российская Федерация; lukin.yury@mail.ru

РЕФЕРАТ
В современном глобальном социуме все более возрастает значимость природных богатств и коммуникаций Арктики. При этом арктическое конфликтное пространство не только не застраховано от кибератак, но их последствия здесь могут быть самыми ужасными в условиях гибридной войны XXI в. Особенно опасными становятся кибератаки на критическую информационную инфраструктуру организаций кредитно-финансовой сферы, экономики, органы власти и управления, другие объекты. Активизируются киберпреступления хакеров с целью получения нелегальных доходов, угрозы утраты денег, имущества населением. Основным источником кибератак на Россию становятся Cyber Command США, возрастают риски обострения кибервойны между США и Россией. Одним из лидеров по защите от киберугроз в Российской Арктике является ПАО «ГМК "Норильский никель"».
Ключевые слова: Арктика, конфликтное пространство, киберугрозы, кибератаки, кибервойна

Problems of Russia's Cyber-Security in the Arctic

Yuri F. Lukin
The Higher School of the Russian Federation, the Academy of Geopolitical Problems, Arkhangelsk, Russian Federation; lukin.yury@mail.ru

ABSTRACT
The importance of Arctic natural resources and communications is increasing in the modern global society. At the same time, the Arctic conflict space is not only unprotected from cyberattacks, but their consequences here can be the most terrible in the hybrid war conditions of the XXI century. Cyberattacks on the critical information infrastructure of credit and financial institutions, the economy, authorities and other facilities are becoming especially dangerous. Cybercrimes of hackers for the purpose of obtaining illegal income, threats of money and property loss by the population become more active. The main source of cyberattacks on Russia are the US Cyber Command, the aggravation risks of cyber warfare between the US and Russia are increasing. One of the leaders in protecting against cyberthreats in the Russian Arctic is PJSC MMC Norilsk Nickel.
Keywords: Arctic, conflict space, cyber threats, cyber-attacks, cyber-war

В глобальной экономике XXI в. все более возрастает значимость Арктики, ее природных богатств, Северного морского пути, арктического природного газа, пресной воды, относительно чистого воздуха. Природная красота Арктики, ее биота привлекает туристов со всего мира. Реализуется проект трансарктического кабеля "Arctic Connect", который свяжет Азию и Европу. В создании надежных подводных информационно-коммуникационных сетей в Арктике, разработке цифровых моделей ведения бизнеса заинтересованы не только Россия, но и Китай, Финляндия, Япония. Подводную высокоскоростную оптическую линию по дну Северного Ледовитого океана протяженностью более 10 тыс. км построят ПАО «МегаФон» и Cinia Oy. Все более последовательно внедряются в практику арктические стандар-

ты, учитывающие специфику хозяйственно-экономической деятельности в Арктике. Российская Арктика очищается от накопленного мусора, постепенно зеленеет экономика. В России внедряются экологически чистые виды водного, железнодорожного, автомобильного транспорта с использованием сжиженного природного газа (СПГ), газозаправочные станции, бункеровочные базы в морских портах, современные технологии генерации энергетики. Все это делает Арктический регион современным, имеющим перспективы дальнейшего развития, для чего, несомненно, необходимо мирное время, инвестиции.

Арктика объективно является стратегически важнейшим регионом мира в военном плане, где высокий уровень военно-политической активности проявляют США, Норвегия, Канада, Дания, Швеция, Россия. О своих претензиях на Арктику заявила даже Великобритания, имеющая статус наблюдателя в Арктическом совете. В Арктике имеются эффективные позиции с точки зрения расстояния и подлетного времени для размещения элементов систем стратегического сдерживания, атомных подводных лодок, для расположения систем ПРО. Российское государство во втором десятилетии XXI в. заметно продвинулось в вопросах обеспечения национальных интересов России в Арктике, своей безопасности.

Уменьшение площади арктических льдов в результате глобального потепления делает северные моря Северного Ледовитого океана сегодня доступными даже для американских авианосцев. Осенью 2018 г. в Норвегии, Финляндии состоялось одно из самых крупномасштабных учений НАТО после 1991 г. “Trident Juncture 2018” («Единый трезубец 2018»), в котором участвовали более 50 тыс. военнослужащих из 31 страны, 65 кораблей, включая американский авианосец «Гарри Трумэн». Руководители НАТО оправдывают военные маневры необходимостью сдерживания России в этом регионе. В СМИ стали появляться возможные сценарии развития военного конфликта в Арктике: перерастание частного экономического противоречия в локальный вооруженный конфликт без последующей эскалации или с последующей эскалацией, внезапная крупномасштабная агрессия, использование слабых сторон России в рамках гибридной войны, кибератак. В данной статье автор не касается угроз военной безопасности РФ в Арктическом регионе, эффективности деятельности ВМФ РФ, Северного флота и других видов вооруженных сил России в Арктике, проблем милитаризации арктического пространства и битвы за Арктику в той или иной форме [4, с. 50–59, 60–732; 5; 10;11].

В XX–XXI вв. пока еще вполне цивилизованно проходит Великий передел Арктики. Однако если ранее в научных публикациях, средствах массовой коммуникации просто высказывались сомнения, будет ли Арктика зоной мира или ареной конфликтов, то примерно с 2014 г. таких сомнений остается все меньше, меняется тональность самих публикаций [2, с. 154–167; 9, с. 244–255]. Л. Г. Ивашов, президент Академии геополитических проблем, вполне обоснованно указывает на перманентные причины глобального противостояния в Арктике, учитывая, что в мире осталось всего три ресурсных района — Арктика, в меньшей степени Афганистан и Антарктида. В Афганистане главное для американцев — контроль над урановыми месторождениями, уран-235 сегодня в дефиците. Углеводородные ресурсы и редкоземельные металлы сосредоточены в Арктике. Американцы хотят принизить роль России в регионе, стать распорядителем и контролером всех арктических ресурсов и морских коммуникаций. XXI в. станет арктической эрой в истории человечества, в ходе которой будет переформатирована нынешняя геополитическая конструкция мира и создана новая. В Арктическом регионе в системе геополитических отношений складывается биполярная модель — Россия и все остальные претенденты. «Американцы, по сути, создают Арктическое НАТО», — отмечал Л. Г. Ивашов еще в 2018 г. [1].

В своих выступлениях, докладах политики, военные в США всю вину за обострение ситуации в Арктике «традиционно» возлагают на Россию. В докладе Дж. Клэппера (James R. Clapper), например, отмечались возрастающие угрозы для США от России, в том числе в Арктике, риск усиления конкуренции между арктическими и неарктическими странами за доступ к морским путям и ресурсам. Прогнозировалось, что Россия почти наверняка продолжит наращивать свое военное присутствие вдоль своего северного побережья, чтобы улучшить защиту периметра и контроль над своей исключительной экономической зоной; будет добиваться международной поддержки своей расширенной претензии на континентальный шельф и своего права управлять движением судов в пределах своей исключительной экономической зоны. В случае дальнейшего ухудшения российско-западных отношений Москва может стать более

склонной дезавуировать сложившиеся международные процессы или организации, касающиеся управления Арктикой, и действовать в одностороннем порядке для защиты этих интересов, — подчеркивалось в анализируемом американском докладе (19.02.2019) [12, с. 13].

Department of Defense (DoD) США опубликовало 6 июня 2019 г. "Report to Congress Department of Defense Arctic Strategy", определивший военную стратегию США для Арктического региона в эпоху конкуренции. Стратегический фокус направлен на конкуренцию с Китаем и Россией как основной вызов долгосрочной безопасности и процветанию США. Доклад "The 2019 DoD Arctic Strategy" определяет три стратегических пути: Building Arctic awareness; Enhancing Arctic operations; Strengthening the rules-based order in the Arctic (создание арктической осведомленности; усиление арктических операций; укрепление основанного на правилах порядка в Арктике). Эти меры требуют срочных инвестиций для модернизации систем обороны в США, улучшения связи и разведки, поддержки миссий береговой охраны, усиления арктических операций, регулярных учений в Арктике, поддержки устойчивой инфраструктуры, укрепления основанного на правилах порядка в Арктике, сотрудничества с союзниками и партнерами для сдерживания агрессии, сохранения свободы морей. Каждое военное ведомство (ВВС, ВМФ, морская пехота, армия, Национальная гвардия) играет важнейшую роль в достижении целей и подходов, изложенных в арктической стратегии. При оценке среды безопасности Арктики в "2019 DoD Arcticstrategy" отмечаются как позитивные, так и проблемные тренды сотрудничества. Хотя непосредственная перспектива конфликта в Арктике, по оценке военного командования США, низкая, эти тренды могут негативно сказаться на нестабильности в регионе. Их динамика определяется ключевыми основными факторами:

1) Changing Physical Environmen (изменения среды);

2) Multilateral Cooperation to Address Shared Interests and Challenges (многосторонняя кооперация для решения общих интересов и проблем);

3) Status of Arctic Sea Routes: Russia and Canada (статус арктических морских путей: Россия и Канада);

4) Increasing Military Activit (рост военной активности);

5) Attempts to Alter Arctic Governance through Economic Leverag (попытки изменить управление Арктикой с помощью системы экономических рычагов). США идентифицируют себя при этом как "Arcticnation" и не признают «никаких других претензий на статус Арктики ни от одного государства, кроме этих восьми государств»[1]. В целом арктическая стратегия США целенаправленно действует против Китая и России, на их сдерживание не только в Арктике, но и в Европе, других регионах мира.

Арктическое пространство в настоящее время объективно остается конфликтным. Конфликты являются естественным состоянием всего глобального социума, любого общества-государства, регионального социума, муниципальной общины, организаций всех типов и форм, в том числе функционирующих в Арктическом регионе. «Не делай другим того, чего не желаешь себе» — это правило Конфуция как нельзя лучше подходит к уникальному пространству Арктики. Но, как и несколько десятков столетий тому назад, этот призыв остается гласом вопиющего в пустыне, всего лишь благим пожеланием в наше сложное и противоречивое время. К конфликтогенным в 2019 г. относились следующие факторы:

a. Дания, Канада, Россия еще не имеют легитимных границ континентального шельфа в акватории СЛО, а США не ратифицировали даже UNCLOS (1982).
b. Отсутствуют общие правила и договоренности о рыболовстве и других формах использования околополюсной области в самом центре СЛО, так называемой зоне ООН, хотя работа в этом направлении ведется.
c. Не отработана правоприменительная практика прохода военных судов иностранных государств по акватории Северного морского пути, используя частично исключительную экономическую зону России, и функционирования Полярного шелкового пути.
d. Принятый в 2017 г. Полярный кодекс пока не исполняется в полном объеме, возможно возникновение конфликтных ситуаций при использовании топлива для судов и по другим экологическим проблемам.

[1] 2019 DoD Arctic Strategy [Электронный ресурс]. URL: https://media.defense.gov/2019/Jun/06/2002141657/-1/-1/1/2019-DOD-ARCTIC-STRATEGY.PDF. P. 1–3 (дата обращения: 10.02.2020).

e. Конфликтные ситуации, связанные с обеспечением безопасности, проведением учений, размещением ракет, АПЛ, военной деятельностью НАТО и России в Арктике.
f. Активизация деятельности Военно-космических сил (ВКС) США с 18 июня 2018 г., поиски асимметричного преимущества (слабого звена) в условиях ведения постоянной кибервойны против России, создание киберугроз, кибератаки, в том числе в Арктике.
g. Обострение информационно-психологической войны против России в СМИ, в международных отношениях по проблемам Арктики: фейки, постправда, провокации, угрозы, политико-экономические санкции, деятельность ВКС США.
h. Не исключаются локальные конфликты по вопросам добычи и переработки нефти и газа, других природных богатств, развития инфраструктуры Арктики, но вопрос о большой войне (Big War) является пока предметом дискуссий[1].
i. В российской Арктике остаются конфликтогенными внутренние социальные, этнокультурные, религиозные отношения, проблемы миграции и качества жизни населения, которые США могут использовать в качестве «слабого звена» в своей стратегии ВКС. В сфере экономики и геополитики преобладает подход к освоению природных богатств Арктики в интересах крупных госкомпаний и ТНК.

Участниками конфликтных ситуаций являются как целые государства, так и организации бизнеса. Даже в самых богатых и крупных российских организациях, работающих в Арктике (Газпром, Роснефть, Новатэк, Росатом, Совкомфлот, Сбербанк и др.), имеющиеся ресурсы ограничены. Необходимость их распределять, регулировать отношения собственности, как показывает практика, неизбежно ведет к возникновению конфликтных ситуаций во всех сферах жизнедеятельности. Конфликты постоянно воспроизводятся в межличностных отношениях между людьми, в семейно-бытовой сфере, различных видах человеческой деятельности. Мы все живем сегодня уже в ином мире, отличном от того, что был в 90-е гг. XX в. или в первом десятилетии XXI в.

Обострение международной ситуации в условиях нарастания киберугроз против России как бы в мирное время может негативно отразиться на реализации национальных проектов, росте экономики и жизнедеятельности населения в Российской Арктике. Военный конфликт в Арктике (Big War) в ближайшее время маловероятен. При этом А. А. Бартош обращает внимание на то, что комплекс угроз для России в Арктике носит гибридный характер и наряду с политико-дипломатическими и военно-силовыми мерами включает разнородные формы и методы информационного и кибернетического воздействия, угрозы от действий террористов и организованной преступности. Сформулирован очень важный тезис: «В Арктике против России ведется гибридная война, что требует соответствующих ''гибридных'' мер противодействия»[2]. В ходе гибридной войны в Арктике каждый из участников реализует свои намерения без непосредственного применения вооруженных сил, без объявления войны. Готова ли Россия к противостоянию в Арктике как бы в «мирных» условиях гибридной войны, сегодня является ключевым вопросом. И речь здесь идет не об очередных масштабных учениях российских АПЛ, десантных кораблей в морях Северного Ледовитого океана или в Атлантике, не о военной мощи Северного флота. Готовы ли наши ВКС, российские организации всех форм и типов к отражению кибератак, минимизации киберугроз в Арктике? К внешним киберугрозам, как известно, относятся DoS/DDoS-атаки, вирусы, спам, фишинг и другие технологии.

И. Ф. Кефели в своих трудах подчеркивает, что **киберпространство** становится доступным для ведения боевых действий — наравне с землей, морем, воздухом и ближним космосом. **В гибридных войнах используется:**

1. Сетевое кибероружие, обеспечивающее доступ многофункциональных компьютерных программ в закрытые внутренние военные и гражданские сети противника, включающие критические объекты.

---

[1] Could the Next Big War Take Place in the Arctic? / by David Axe. 11.03.2019. Russia in the Arctic: Friend or Foe? / By Jennifer Loy. [Электронный ресурс]. URL: https://www.geopoliticalmonitor.com/russia-in-the-arctic-friend-or-foe/ (дата обращения: 10.02.2020).

[2] *Бартош А. А.* Гибридная война в Арктике // Мировая политика. 2018. № 3. С. 59–73. [Электронный ресурс]. URL: http://e-nota-bene.ru/wi/article_21010.html (дата обращения: 14.11.2019).

2. Коммуникационное кибероружие, которое представляет собой программный код, способный искажать и блокировать обмен сигналами между удаленным оператором и боевым роботом.
3. Предустановленное кибероружие, в элементную базу которого производителем закладывается управляющий софт с различного рода «логическими бомбами», способными выводить из строя кибероружие под воздействием внешних сигналов.
4. Проникающее кибероружие, базирующееся на целенаправленном изменении различных физических сред (акустической, оптической и др.), которое приводит к модификации сигналов, поступающих на внешние сенсорные датчики высокотехнологичных вооружений и приводящих к их выходу из строя.
5. Электромагнитное оружие, полностью выводящее из строя в ходе превентивного удара боевую технику, «выжигая» элементную базу наступательного вооружения противника. **В мирное время кибероперации — это диверсии, теракты, идеологическая обработка гражданского населения**. Информационно-психологическая война охватывает внутренний мир человека, его инстинкты, психику, чувства, эмоции, мысли, мировоззрение, индивидуальное и общественное сознание [3, с. 232–242].

Гибридная война в Арктическом регионе реально включает сегодня киберпространство, информационную, психологическую, правовую составляющие, дипломатию; целевое распространение фейков (ложной информации) в СМИ, ТВ, кино, искусстве; постоянное воздействие на культуру, менталитет населения; экономическое давление, взаимные угрозы и обвинения в сфере международного и национального права по вопросам использования Северного морского пути, границ арктического шельфа, экологии, рыболовства и другим. Политические и экономические санкции со стороны США и Европейского союза вводятся против людей, бизнеса, организаций, работающих в Российской Арктике. В системе гибридных войн против государств, народов и мировых цивилизаций широко используется «мягкая сила» [6]. Военное противостояние усиливается в форме роста бюджетов арктических государств США, Российской Федерации, Канады, Норвегии на обеспечение безопасности, военные учения, модернизацию вооружений, разработку военных доктрин. На таком геополитическом фоне особенно опасными в мирное время без всякого преувеличения становятся кибератаки, в том числе на энергетику, финансово-кредитные организации, крупные облачные хранилища[1].

В России Национальный координационный центр по компьютерным инцидентам (далее — НКЦКИ) был создан 24 июля 2018 г. В Положении о НКЦКИ говорится о том, что Центр организует и осуществляет обмен информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры, в том числе на международном уровне; осуществляет сбор, хранение и анализ информации о компьютерных инцидентах и компьютерных атаках, а также анализ эффективности мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.

Российская Арктика, как и любой другой регион мира, не застрахована сегодня от кибератак по самым разным поводам на информационные ресурсы (ИР) и критическую информационную инфраструктуру (КИИ). Нельзя забывать, что еще в последнем десятилетии прошлого века в ходе широких дискуссий и работы появились такие термины, как «кибервойна», High Modern War, «война космической эры», «гиперсовременная война», «война эпохи умных машин», «информационная война». Новая парадигма войны рассматривалась не только с узкоутилитарной позиции, но и в связи с философией, культурной антропологией и социологией, с охватом киберпространства + медиа. Не обязательно полностью уничтожать вооруженные силы или инфраструктуру, нужно лишь правильно и точно рассчитать, какие именно центры и в какой момент следует подвергнуть атаке, подчеркивал в те годы полковник ВВС США Джон Уорден. Электроэнергетические потери будут иметь разрушительное воздействие на стратегическую основу, что сделает ведение войны чрезвычайно трудным. Уорден обосновал концепцию об уязвимых центрах тяжести, о том, что любая страна среднего размера при поражении до пятисот ее объектов

[1] В России зафиксировали крупную кибератаку на кредитно-финансовые структуры. Эксперты определили основные объекты кибератак в 2019 г. Раскрыты подробности первой кибератаки США на Россию [Электронный ресурс]. URL: https://lenta.ru/news/2019/02/28/no_fun/ (дата обращения: 11.03.2019).

может быть полностью парализована (Warden J. The Enemy as a System. Airpower Journal, Spring 1995) [8, с. 12, 14–15]. Фактически эти идеи были апробированы в ходе боевых действий в Ираке, Сомали, Боснии, Югославии. Среди асимметричных подходов, включаемых в стратегию непрямого воздействия на противника, следует отметить "Net-Centric Warfare" — это сугубо военная концепция, повлиявшая на изменение инфраструктуры Пентагона, а также военную стратегию США. "Netwar" также связана с императивами информационной эры, постмодерна и глобализации.

Американские спецслужбы уже не первый год обвиняют российских хакеров якобы во внедрении в американские системы, в том числе энергетические, опасного программного обеспечения. В 2008 г. Россия как бы проникла в секретные сети связи Пентагона, и это привело к созданию киберкомандования США. В конце первого президентского срока Обамы официальные лица начали сообщать о русской хакерской группе, известной частным исследователям в области безопасности под названием "Energetic Bear и Drag on fly". Данная хакерская группа якобы взломала в 2014 г. обновления программного обеспечения сотен систем, имеющих доступ к управлению электроснабжением. Сообщалось также о кибератаке на западе Украины в декабре 2015 г. (In December 2015, a Russian intelligence unit shut off power to hundreds of thousands of people in western Ukraine.) Все эти и другие обвинения подобного рода требуют убедительных доказательств. Возникает вопрос: фейки это, явная ложь или полуправда? Президент США Д. Трамп обвинил, например, газету "New York Times" в государственной измене, что публикация дезинформирует общественность.

На самом деле в США, согласно публикации в газете "The New York Times" 15 июня 2019 г., по словам действующих и бывших государственных чиновников, действия в отношении кибербезопасности российских энергетических сетей проводятся по меньшей мере с 2012 г. Однако в последнее время стратегия приобрела более наступательный характер и включает в себя размещение вредоносного программного обеспечения внутри российской системы на такой глубине и с такой агрессивностью, которые раньше никогда не применялись. Активизировали цифровые вторжения в российскую электроэнергетическую систему в качестве предупреждения президенту Владимиру Путину и демонстрации того, как администрация Трампа использует новые власти для более агрессивного развертывания киберинструментов[1]. В соответствии с документом «Президентский меморандум о национальной безопасности 13» (NSPM, 2018), Президент США делегировал генералу Полу М. Накасоне гораздо больше свободы действий для проведения наступательных онлайн-операций без получения одобрения президента. Группа Совета национальной безопасности работает над реализацией киберстратегии администрации Трампа в космосе. Киберкомандование США более тесно работает с энергетическим сектором и Министерством энергетики в случае злонамеренной или катастрофической кибератаки. Команды CNMF наблюдают за конкретными противниками и работают над тем, чтобы атаковать этих игроков, прежде чем они достигнут американского киберпространства.

Если Рубикон действительно перейден, то угрозы кибератак рискуют перерасти в ежедневную холодную войну в киберпространстве между Вашингтоном и Москвой [7]. В этой войне принимают участие Китай и другие страны. В 2017 г. министры обороны Европейского союза приняли участие в первой в истории союза кибертренировке, во время которой они отвечали на имитацию хакерской атаки на одну из военных миссий блока за рубежом[2]. Кибератаки становятся главной частью гибридной войны, включающей также информационную, психологическую составляющие, сетевые войны.

Российская Арктика не только не застрахована от кибератак, сетевых войн, но их последствия здесь могут быть самыми ужасными в условиях гибридной войны XXI в. Трудно даже представить те негативные последствия, которые могут наступить в результате кибератак на атомные АЭС в Мурманске, Певеке, объекты теплоснабжения, расположенные в Российской Арктике. Значительный ущерб могут нанести киберпреступления с целью получения нелегальных доходов, которые несут угрозы утраты денег, имущества, квартир любому гражданину, особенно людям старших поколений, недостаточно приспособленных к использованию цифровых технологий.

---

1 U.S. Escalates Online Attacks on Russian's Power Grid. By *David E. Sanger* and *Nicole Perlroth* // The New York Times. June 15, 2019.

2 ЕС проведет «военные игры» для подготовки к кибератакам из России и Китая [Электронный ресурс]. URL: https://www.unian.net/science/10600083-es-provedet-voennye-igry-dlya-podgotovki-k-kiberatakam-iz-rossii-i-kitaya.html (дата обращения: 11.03.2019).

Задача добыть информацию, содержащуюся в цифровой форме, стоит сегодня как перед вполне легальными сотрудниками спецслужб и разработчиками программного обеспечения, так и перед киберпреступниками — людьми, которые крадут данные с целью наживы, превратили этот промысел в свой бизнес, включая естественно и Арктический регион. Современное хакерское сообщество глобального социума состоит из 14 объединений, имеющих четкую специализацию, связанных между собой в Интернете и Даркнете (см. рисунок).

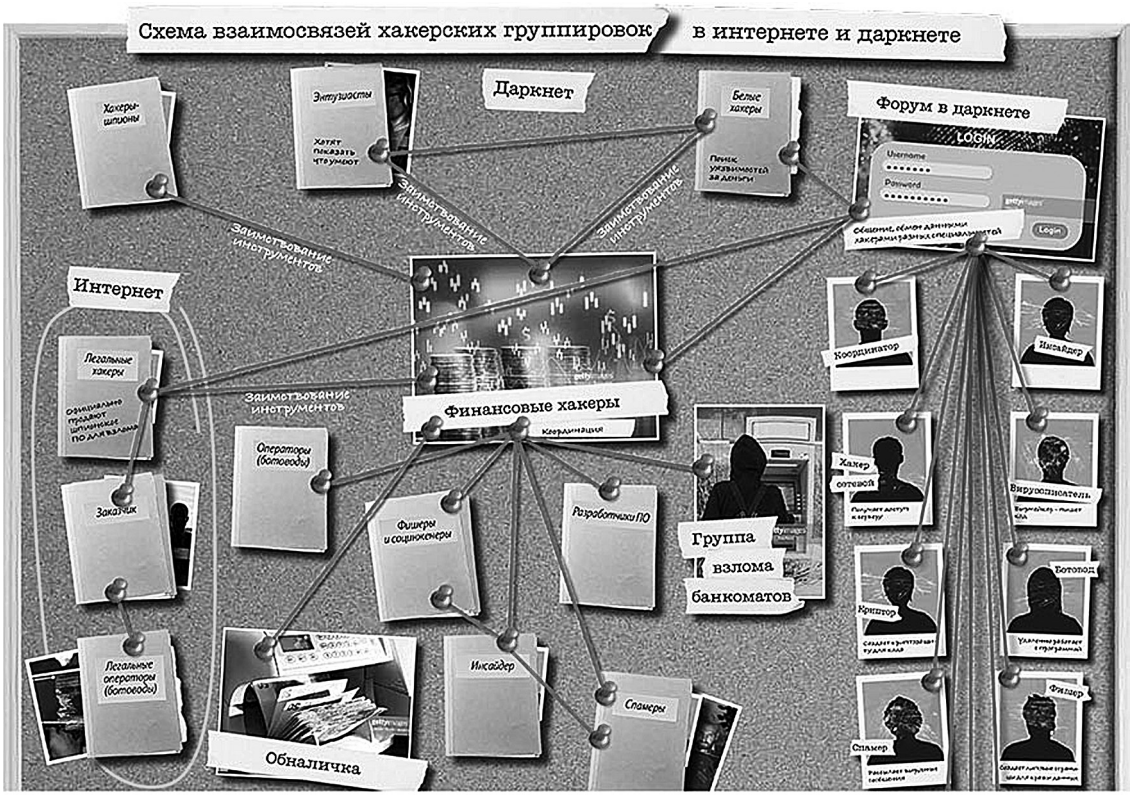

Рис. Хакерское сообщество глобального социума[1]

DarkNet — темный слой Интернета, обеспечивающий более высокую степень анонимности. В нем сконцентрированы сообщества, занимающиеся незаконной деятельностью — торговлей оружием, наркотиками, банковскими картами. В лаборатории Касперского посчитали, что количество хакеров, ведущих свою деятельность в настоящий момент по всему миру, достигает десятков тысяч, в том числе высококвалифицированные программисты, которые обладают серьезным техническим обеспечением, могут находить неустраненные уязвимости, против которых еще не разработаны защитные механизмы. Самая крупная по числу участников группировка занимается финансовыми киберпреступлениями, а самая технически оснащенная — группа создателей шпионских программ[2].

Вице-президент по информационной безопасности ПАО «Ростелеком» И. В. Ляпунов обобщает, что количество кибератак в России в 2018 г. увеличилось почти вдвое, а бюджет российской «скрытой сети» и хакеров превысил 2 млрд руб. Он отмечал как массовый характер кибератак, так и целевые таргетированные атаки, направленные на получение денег. 75% кибератак затрагивают финансовые

[1] [Электронный ресурс]. URL: https://www.toprunews.com/wp-content/uploads/2019/04/175.jpg (дата обращения: 11.03.2019).
[2] [Электронный ресурс]. URL: https://news.myseldon.com/ru/news/index/210368987 (дата обращения: 29.04.2019).

организации, интернет-торговлю, игровой бизнес, а в последнее время целью атак становятся инфраструктурные объекты. За последние полтора года проявилась очень серьезная тенденция — сейчас достаточное количество целевых атак направлены на критическую информационную инфраструктуру: системы управления опасными производствами, системы жизнеобеспечения, системы государственного управления. Возник термин «политически мотивированных атак»: «Цель атакующих — это получение контроля и точки присутствия в этой критической информационной инфраструктуре»[1].

Таким образом, кибератаки на Россию создают в настоящее время конфликтное киберпространство, затрагивая Арктику. В настоящее время Арктика объективно становится перманентным конфликтным киберпространством, в том числе объектом политически мотивированных кибератак на критическую информационную инфраструктуру. Кроме этого, активизируются киберпреступления хакеров с целью получения нелегальных доходов, которые несут угрозы утраты денег, имущества населением Российской Арктики.

Литература

1. *Ивашов Л.* Разворачивается глобальное противостояние за обладание арктическими ресурсами. 23 октября 2018 г. [Электронный ресурс]. URL: https://izborsk-club.ru/16019 (дата обращения: 02.02.2020)].
2. *Карякин В. В.* Природные ресурсы Арктики — источник конфликтогенности и вызовов региональной стабильности // Обеспечение национальных интересов России в Арктике: Труды НИО Института военной истории. Т. 9. Кн. 1. СПб, 2014.
3. *Кефели И. Ф.* Информационно-психологическое противоборство в киберпространстве: геополитический ракурс // Новые горизонты глобального мира : сб. науч. трудов. Балт. гос. техн. ун-т. СПб., 2015.
4. *Королев В. И.* Военно-морская деятельность России в Арктике // Обеспечение национальных интересов России в Арктике: Труды НИО Института военной истории. Т. 9. Кн. 1. СПб, 2014.
5. *Криницкий Ю.* ВКС России в борьбе за Арктику // Журнал ВКС. 2016, декабрь. № 3–4 (88–89).
6. Мягкая сила в международных отношениях : сб. науч. трудов под редакцией Л. Г. Ивашова. М., 2018. 290 с.
7. *Подругина В., Вавина Е., Петлевой В.* Спецслужбы США готовятся к атакам на российские энергетические сети // Ведомости. 2019. 16 июня.
8. *Савин Л. В.* Сетецентричная и сетевая война. Введение в концепцию. М. : Евразийское движение, 2011.
9. *Янг О. Р.* Арктика в будущем: арена конфликтов или зона мира? Обзор публикаций // Вестник Москов. ун-та. Серия 25. Международные отношения и мировая политика. 2011. № 2.
10. Areas of (no) Conflict in the Arctic. Published at: Apr 24. 2018 / From Kathrin Stephen [Электронный ресурс]. URL: https://www.highnorthnews.com/en/areas-no-conflict-arctic (дата обращения: 24.08.2018)].
11. Military Capabilities in the Arctic: a New Cold War in the High North? / Siemon T. Wezeman. SIPRI Background Paper. October 2016. 24 p.
12. Worldwide Threat Assessment of the US Intelligence Community / James R. Clapper, Director of National Intelligence. February 9, 2016. P. 13.

Об авторе:

Лукин Юрий Федорович, профессор, доктор исторических наук, заслуженный работник высшей школы Российской Федерации, действительный член Академии геополитических проблем (Архангельск, Российская Федерация); lukin.yury@mail.ru

[1] [Электронный ресурс]. URL: https:// interesnoe.me/source-72009603/post-4496384 (дата обращения: 18.04.2019).

References

1. *Ivashov L.* Razvorachivaetsya global'noe protivostoyanie za obladanie arkticheskimi resursami. 23 oktyabrya 2018 g. [Elektronnyi resurs]. URL: https://izborsk-club.ru/16019 (data obrashcheniya: 02.02.2020)].
2. *Karyakin V. V.* Prirodnye resursy Arktiki — istochnik konfliktogennosti i vyzovov regional'noi stabil'nosti // Obespechenie natsional'nykh interesov Rossii v Arktike: Trudy NIO Instituta voennoi istorii. T. 9. Kn. 1. SPb, 2014.
3. *Kefeli I. F.* Informatsionno-psikhologicheskoe protivoborstvo v kiberprostranstve: geopoliticheskii rakurs // Novye gorizonty global'nogo mira : sb. nauch. trudov. Balt. gos. tekhn. un-t. SPb., 2015.
4. *Korolev V. I.* Voenno-morskaya deyatel'nost' Rossii v Arktike // Obespechenie natsional'nykh interesov Rossii v Arktike: Trudy NIO Instituta voennoi istorii. T. 9. Kn. 1. SPb, 2014.
5. *Krinitskii Yu.* VKS Rossii v bor'be za Arktiku // Zhurnal VKS. 2016, dekabr'. № 3–4 (88–89).
6. Myagkaya sila v mezhdunarodnykh otnosheniyakh : sb. nauch. trudov pod redaktsiei L. G. Ivashova. M., 2018. 290 s.
7. *Podrugina V., Vavina E., Petlevoi V.* Spetssluzhby SShA gotovyatsya k atakam na rossiiskie energeticheskie seti // Vedomosti. 2019. 16 iyunya.
8. *Savin L. V.* Setetsentrichnaya i setevaya voina. Vvedenie v kontseptsiyu. M. : Evraziiskoe dvizhenie, 2011.
9. *Yang O. R.* Arktika v budushchem: arena konfliktov ili zona mira? Obzor publikatsii // Vestnik Moskov. un-ta. Seriya 25. Mezhdunarodnye otnosheniya i mirovaya politika. 2011. № 2.
10. Areas of (no) Sonflict in the Arctic. Published at: Apr. 24 2018 / From Kathrin Stephen [Elektronnyi resurs]. URL: https://www.highnorthnews.com/en/areas-no-conflict-arctic (data obrashcheniya: 24.08.2018)].
11. Military Capabilities in the Arctic: a New Cold War in the High North? / Siemon T. Wezeman. SIPRI Background Paper. October 2016. 24 p.
12. Worldwide Threat Assessment of the US Intelligence Community / James R. Clapper, Director of National Intelligence. February 9, 2016. P. 13.

About the author:

Yuri F. Lukin, Professor, doctor of historical Sciences, Honored Worker of the Higher School of the Russian Federation (Arkhangelsk, Russian Federation), Full Member of the Academy of Geopolitical Problems; lukin.yury@mail.ru