ТЕОРЕТИЧЕСКИЕ ПОИСКИ И ПРЕДЛОЖЕНИЯ

THEORETICAL SEARCH AND OFFERS

Вестник НГУЭУ. 2023. № 1. С. 206–221
Vestnik NSUEM. 2023. No. 1. P. 206–221

Научная статья
УДК 351
DOI: 10.34020/2073-6495-2023-1-206-221

ЦИФРОВАЯ ВОЙНА: ПОНЯТИЕ, ГЕНЕЗИС, ПРОБЛЕМЫ ЗАЩИТЫ НАЦИОНАЛЬНЫХ ИНТЕРЕСОВ ГОСУДАРСТВ

Ермаков Антон Сергеевич

ООО «Инсейлс Рус»
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации

ermakov4work@gmail.com

Аннотация. Цифровая война является эволюционно новым этапом реализации военных интересов государства путем трансмиссии военных действий в цифровое пространство. На сегодняшний день в России сформирована и продолжает развиваться централизованная модель управления информационной безопасностью в цифровой экономике, что укладывается в уже отлаженную вертикально интегрированную модель государственного управления, однако важная черта ее эффективного функционирования – необходимость глубокого проникновения в информационное окружение каждого из граждан, бизнесов и некоммерческих организаций, а это приводит к паническим настроениям в обществе и еще сильнее усиливает нестабильность информационного периметра государства и повышает риски ослабления цифрового суверенитета.

Ключевые слова: цифровая война, информационная безопасность, организованные кибератаки, уязвимость, цифровой суверенитет, критическая инфраструктура

Для цитирования: Ермаков А.С. Цифровая война: понятие, генезис, проблемы защиты национальных интересов государств // Вестник НГУЭУ. 2023. № 1. С. 206–221. DOI: 10.34020/2073-6495-2023-1-206-221.

Original article

DIGITAL WARFARE: CONCEPT, GENESIS, PROBLEMS OF DEFENSE OF NATIONAL INTERESTS OF STATES

Ermakov Anton S.

Insales Rus LLC
Russian Presidential Academy of National Economy and Public Administration

ermakov4work@gmail.com

Abstract. Digital warfare is an evolutionarily new stage in the realization of state military interests by transmitting military actions into the digital space. To date, Russia has formed and continues to develop a centralized model of information security management in the digital economy, which fits into an already well-established vertically integrated model of public administration, but an important feature of its effective functioning is the need for deep penetration into the information environment of each citizen, businesses and non-profit organizations, and this leads to panic moods in society and further increases the instability of information.

Keywords: digital warfare, information security, organized cyber-attacks, vulnerability, digital sovereignty, critical infrastructure

For citation: Ermakov A.S. Digital warfare: concept, genesis, problems of defense of national interests of states. *Vestnik NSUEM*. 2023; (1): 206–221. (In Russ.). DOI: 10.34020/2073-6495-2023-1-206-221.

Введение. «Темной стороной» цифровой экономики является ее бескомпромиссная политика стирания физических границ между индивидами, бизнесами и целыми государствами, миссией которой является создание единого информационного пространства планетарного масштаба. Однако, несмотря на весь научно-технический прогресс и эволюцию устройства социально-экономических отношений в пользу ответственного отношения к окружающей среде, толерантности и миролюбивости, соперничество и борьба являются неотъемлемыми компонентами жизненного цикла политической элиты любого государства, и по сути «…продолжением политики иными средствами» [5, с. 11]. Высшей формой проявления борьбы в государстве является война, с наступлением эпохи Индустрии 4.0 механизм осуществления и формат протекания которой перестал быть явным, перейдя в невидимую сторону цифрового, виртуального мира, но не став от этого менее опасным или разрушительным.

Вообще фундаментальные постулаты цифровой экономики оказались благодатной почвой для формирования новых форм и ценностных установок возникновения конфликтов, потенциально могущих стать полноценной войной: во-первых, цифровая экономика прямо декларирует стремление к информационной открытости и прозрачности всех акторов социально-экономических отношений, что вызывает не только опасения за конфиденциальность персональных данных, но и создает многочисленные угрозы для манипулирования интересами как отдельных лиц, так и общества в целом; во-вторых, двигателем развития цифровой экономики является бесшовная

интеграция акторов всех уровней не только в границах одного государства, но и мира в целом, что несет в себе уже риски стирания национального суверенитета и возможности защищать свои национальные интересы; в-третьих, цифровая экономика жестко обнажает существующие разрывы в уровне научно-технологического развития стран, приводя к их стратификации, а в будущем – возникновению кастовости, которая определяет будущее целых государств и их положение на международной арене. Все это подчеркивает *актуальность темы научного исследования* и ее *практическую значимость* для обеспечения устойчивого развития России и защиты ее национальных интересов в условиях эскалации санкций и попыток международной изоляции.

Целью научной статьи является аналитическая оценка киберинцидентов в цифровом пространстве Российской Федерации и оценка их влияния на цифровую экономику в целом.

Объектом научного исследования является цифровая война как новая разновидность высшей формы проявления конфликта интересов политических элит государства. *Предметом* научного исследования являются киберинциденты, происходящие в формирующейся цифровой экономике России.

Научная статья носит междисциплинарный характер и охватывает экономические (развитие цифровой экономики, инвестиции в кибербезопасность, уровень инновационной активности бизнеса), технологические (защищенность объектов критической инфраструктуры, количество киберугроз и кибератак) и политические (проблема защиты цифрового суверенитета и международного правового регулирования кибервойны) аспекты цифровой войны.

Подготовка научного исследования осуществлялась с использованием *общенаучных* (наблюдение, сравнение, измерение, анализ и синтез, метод логического рассуждения) и *специальных* (статический анализ, экспертные оценки, графический метод) методов. Обоснованность и достоверность результатов научного исследования обеспечивается корректностью и строгостью построения логики и схемы исследования, а также использованием верифицированной статистической информации из публичных материалов Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России[1], тематические отчеты «Кибербезопасность. Тренды и прогнозы» PT Security[2], консалтингового агентства PWC (Глобальное исследование Digital Trust Insights 2021[3]).

Научная новизна публикации заключается в формировании качественного аналитического обзора киберинцидентов в формирующейся цифровой экономике России в 2017–2021 гг. и выявлении по его результатам ключевых киберуязвимостей и рекомендаций по их устранению для эффективной защиты цифрового суверенитета государства.

[1] ФинЦЕРТ: официальный сайт Банка России. [Электронный ресурс]. URL: https://cbr.ru/information_security/fincert/.

[2] Positive Technologies: официальный сайт. [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/.

[3] Глобальное исследование Digital Trust Insights 2021. [Электронный ресурс]. URL: https://www.pwc.com/kz/ru/services/global-digital-trust-insights.html.

Обзор литературы и исследований. Исходной точкой научного исследования является формирование понятийного аппарата: определение термина «цифровая война» в отечественной и зарубежной академической литературе. Однако даже беглый критический обзор показал многообразность понятий, синонимизированных с объектом научного исследования: «кибертерроризм», «цифровой террор», «гибридная война», поэтому принимая во внимание междисциплинарный характер исследования, сложность и глубину регулятивно-правового блока идентификации конфликта именно как война в различных юрисдикциях, было решено сделать понятийно-разъяснительную вставку, позволяющую разграничить родственные по смыслу и целям понятия.

Итак, под терроризмом, по мнению А.К. Кронина (A.K. Cronin) [12], Дж.П. Гиббса (J.P. Gibbs) [14] и Г. Эванса (G. Evans) [13], понимается действие отдельного лица или группы лиц, направленное на привлечение внимания общественности и политической элиты, запугивание или принуждение гражданского населения, влияние на государственную политику через совершение противоправного деяния, несущего значительную общественную опасность и не подчиняющуюся установленным правилам и обычаям войны.

Исходя из приведенного выше определения понятия «терроризм», *кибертерроризм* можно трактовать как противоправное воздействие лица или группы лиц на информационную инфраструктуру с целью дестабилизации ее функционирования или получения возможности манипулятивного управления ее работой, несущей угрозы причинения вреда жизни, здоровью или имуществу неопределенного круга лиц [3, 4]. Таким образом, в отличие от цифровой войны это понятие характеризует частные деструктивные проявления лиц, имеющих крайние взгляды и не способные (не готовые) к ведению диалога с действующей архитектурой государственного управления, т.е. их проявление как правило пространственно ограничено конкретным государством, реже – группой стран.

Цифровой террор является более высоким по уровню организации и проявления понятием и связан с интересами политических элит и доступными им инструментами управления силовым блоком (армия, правоохранительные органы) и функционированием критической инфраструктуры (системы связи, транспортная и банковская инфраструктура). В понимании Ф. Убстера и Ф. Хайека, *цифровой террор* – это комплекс мер и инструментов, организованных политической элитой в единый механизм манипулятивного воздействия на общество с целью подчинения частных интересов и поведенческих паттернов национальным целям и задачам, а также формирования тотального контроля за гражданами [7, 8]. Цифровой террор *всегда является сознательным выбором политической элиты государства*, применяемый ею для достижения целей и (или) решения задач. В некоторых случаях, по мнению К. Хеджеса, такая форма может быть применена как защитная реакция на растущие внешние вызовы и угрозы, могущие привести к потере суверенитета или разрушению существующей архитектуры политического устройства [9, с. 149–150].

Лучшее, по мнению автора, определение понятия «*гибридная война*» содержится в военном справочнике Military Balance: «использование воен-

ных и невоенных инструментов в интегрированной кампании, направленной на достижение внезапности, захват инициативы и получение психологических преимуществ, использующих дипломатические возможности; масштабные и стремительные информационные, электронные и кибероперации; прикрытие и сокрытие военных и разведывательных действий в сочетании с экономическим давлением» [6, с. 33].

Как следует из приведенной выше вставки, цифровая война является «ближайшим родственником» к гибридной войне, но отличается от нее более высоким уровнем самоорганизации и сущностно-функциональной автономностью, удаленностью от места протекания, так как может вестись самостоятельно без прибегания к использованию вооруженных сил. Исходя из выявленных особенностей, автором был подготовлен свод определений термина «цифровая война» в отечественной и зарубежной академической литературе (табл. 1).

Таблица 1

Определение термина «цифровая война» в отечественной и зарубежной академической литературе

Definition of the term “digital war” in domestic and foreign academic literature

Автор (-ы) / Источник	Содержание определения / *особенности трактовки*
1	2
I. *Отечественная литература*	
1. Н.А. Чернышенко [10, с. 37–38]	Масштабное удаленное вмешательство представителей одного государства в интересы другого путем использования информационно-компьютерных технологий для нарушения нормального протекания социально-экономических процессов в обществе и подрыва доверия граждан к государственным институтам управления *Особенности трактовки:* определение не раскрывает подробностей содержания кибервойны как высшей формы конфликта, а только указывает на использование в рамках ее ведения информационно-компьютерных технологий и удаленный характер одной из сторон-участников
2. М.Е. Бегларян, Я.Н. Войтова-Долгих, С.А. Одинцов [2, с. 13–14]	Санкционированное уполномоченными лицами государственного управления применение специальными силами одного государства информационно-компьютерных технологий и сети Internet для нанесения ущерба физическим объектам критической инфраструктуры в другом государстве без прямой физической интервенции на его территорию *Особенности трактовки:* в определении четко обозначен один из важнейших объектов кибервойны – физическая критическая инфраструктура, обеспечивающая нормальное и стабильное функционирование общества и государства, подчеркивается отсутствие «физического контакта» сторон
3. Н.А. Балаклеец [1, с. 140]	Совокупность мер и действий государства-агрессора, цель которых сформировать в атакуемом государстве перманентное чрезвычайное положение, что в свою очередь приводит к внутренним волнениям, хаосу и паническим настроениям общественности, и истощению внутренних ресурсов, связанных с неопределенностью дальнейшего развития событий

Окончание табл. 1

1	2
	Особенности трактовки: понятие рассматривается через призму долгосрочной программы действий участника-агрессора, направленного на «ресурсное и психологическое истощение» противника с использованием комплекса информационно-коммуникационных технологий
II. *Зарубежная литература*	
1. Т. Хольт (T. Holt) [16, с. 214–215]	Некодифицированная в международном законодательстве форма конфликта, выражающаяся в деструктивных действиях некоторых лиц (сил) против цифрового суверенитета другого государства или его отдельных институтов *Особенности трактовки:* в данном определении делается важный акцент на некодифицированном характере формы кибервойны, указывающий на широкий характер ее влияния и множественность инструментов, которые могут использоваться
2. Экспертная группа по кибервойнам RAND Corporation	Конфликт правительств и международных организаций против других правительств, направленный на уничтожение информационной и компьютерной сети[4] *Особенности трактовки:* в определении подчеркивается ориентация кибервойны на разрушение информационной инфраструктуры в стране-противнике
3. Р.Ж. Харкнет, М. Смит (R.J. Harknett, M. Smeets) [15], Ф. Кристиано (F. Cristiano) [11]	Эволюционно новый этап реализации военных интересов государства путем перевода традиционных военных операций в цифровое (виртуальное) пространство с привлечением частных высокотехнологичных бизнесов и специалистов в области несанкционированного доступа в информационные системы (хакеров)

Источник: авторская разработка.

Согласно приведенному компаративному анализу суждений, для российских ученых характерна более узкая, ближе к кодифицированной, трактовка термина, что обусловлено рядом причин: 1) для РФ активная фаза цифровизации национальной экономики началась в 2017 г. с принятием Национальной программы «Цифровая экономика Российской Федерации»[5], т.е. имеет место некоторое запоздание по сравнению с мировыми лидерами развития институтов цифровой экономики; 2) имеющая место узость трактовки термина существенно усложняет идентификацию происходящих кибератак, массовых хакерских вторжений и их категориальное отнесение, так как часть из них имеет доказательства участия недружественных государств[6].

[4] Cyber Warfare. [Электронный ресурс]. URL: https://www.rand.org/topics/cyber-warfare.html.

[5] Национальная программа «Цифровая экономика Российской Федерации»: распоряжение Правительства № 1632-р от 28.07.2017 г. [Электронный ресурс]. URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf.

[6] Белый дом подтвердил проведение «кибероперацій» против России (02.06.2022). [Электронный ресурс]. URL: https://www.rbc.ru/politics/02/06/2022/6297d5699a7947622ed04206.

В зарубежной практике, напротив, имеет место более широкое понимание термина и включение в его состав инструментов, которые официально никогда не будут санкционированы соответствующими институтами власти (например, хакерские атаки), что обусловлено закреплением в военной доктрине концепции ведения цифровой войны: например, руководством США в 2018 г. принята новая редакция документа «Национальная стратегия кибербезопасности»[7], в котором закреплен механизм ведения кибервойны; в ЕС такой механизм описан в документах: «Таллинское руководство по применению международного права к кибероперациям»[8] (2017 г.) и «Акт о кибербезопасности» (Cybersecurity Act)[9] (2019 г.). *Во-первых*, в странах коллективного Запада имеет место более высокий уровень цифровой зрелости бизнеса и его сетевая связанность между собой, что многократно повышает киберугрозы для его нормального функционирования; *во-вторых*, в настоящее время в мире выделяют два мощных центра киберсил: группа компаний FAMGA (США) и BAT (Китай), которые не только обладают достаточным потенциалом для ведения полноценной кибервойны, но и находятся в перманентном противостоянии друг с другом и активно совершают провокационные и вредительские акты в информационном поле стран-противников[10]. *В-третьих*, страны СНГ в целом и РФ в частности являются технологически зависимыми от высокотехнологичных продуктов стран Запада (по данным за 2020 г. уровень технологической зависимости составил от 47,0 до 65,0 %[11]).

Результаты. Следующим этапом научного исследования являются анализ ключевых индикаторов и метрик произошедших киберинцидентов в цифровом пространстве РФ в 2017–2021 гг. и оценка их влияния на цифровую экономику в целом. Принимая во внимание отсутствие в национальном законодательстве закрепленного термина «цифровая война», при сборе данных автором анализировался индикатор «организованные кибератаки», которые принимаются экспертами профильных компаний в сфере информационной безопасности для обозначения атак, ведущих к организованным структурам: национальные и международные хакерские группы, правительственные организации, частные военные корпорации в сфере информационных технологий, чье участие является доказанным для возбуждения уголовного дела и инициации расследования (табл. 2).

[7] Новая стратегия кибербезопасности США: краткий анализ новой редакции (16.10.2018). [Электронный ресурс]. URL: http://csef.ru/ru/oborona-i-bezopasnost/272/novaya-strategiya-kiberbezopasnosti-ssha-kratkij-analiz-novoj-redakczii-8665.

[8] Таллинское руководство 2.0 и захват киберпространства (06.02.2017). [Электронный ресурс]. URL: https://www.geopolitica.ru/article/tallinskoe-rukovodstvo-20-i-zahvat-kiberprostranstva (дата обращения: 26.12.2022, доступ: свободный).

[9] Акт ЕС о Кибербезопасности (Cybersecurity Act) (17.12.2019). [Электронный ресурс]. URL: https://medium.com/lawgeek-by-aurum/eu-cybersecurity-act-review-aurum-law-firm-d588db539e75.

[10] Кибервойна США и Китая продолжается: обнаружена элитная китайская группа со связями в спецслужбах (04.10.2022). [Электронный ресурс]. URL: https://www.securitylab.ru/news/534208.php.

[11] Индикаторы инновационной деятельности: 2022: статистический сборник / Н.В. Городникова, Л.М. Гохберг, К.А. Дитковский и др.; Нац. исслед. ун-т «Высшая школа экономики». М.: НИУ ВШЭ, 2022. С. 24–25; 52–53; 92–93; 109–114; 167–181; 200.

Таблица 2

Ключевые индикаторы и метрики киберинцидентов в цифровом пространстве РФ в 2017–2021 гг. и оценка их влияния на цифровую экономику в целом[12–17]

Key indicators and metrics of cyber incidents in the digital space of the Russian Federation in 2017–2021 and assessment of their impact on the digital economy as a whole

Индикаторы / метрики	2017 г.	2018 г.	2019 г.	2020 г.	2021 г.
1. Общее количество идентифицированных организованных кибератак, всего, ед.	1179	1264	1508	2271	2418
2. Структура атакуемых институтов, % к итогу	100,0	100,0	100,0	100,0	100,0
2.1. Государственные учреждения	14,5	12,8	14,6	15,6	20,4
2.2. Промышленность	20,8	18,1	12,8	10,3	11,3
2.3. Ритейл	20,6	12,6	16,4	18,1	6,5
2.4. Критическая инфраструктура	20,4	22,8	23,5	20,8	27,2
2.5. Финансовые институты	23,7	33,7	32,7	35,2	34,6
3. Оценочные потери национальной экономики от кибератак, млрд руб.	>116	600	2500	>3500	>7000
4. Уровень защищенности национальной экономики от кибератак, % к итогу (*расчет по методологии пентестов PT Research в основных отраслях*)[18]	100,0	100,0	100,0	100,0	100,0
4.1. Критически низкий / низкий	45,9	40,6	37,3	32,5	27,7
4.2. Удовлетворительный	14,8	16	12,4	10,7	9,7
4.3. Достаточный	28,7	30,3	34,6	37,9	40,2
4.4. Высокий	10,6	13,1	15,7	18,9	22,4
5. Уровень организованности кибератак по типу участников, % к итогу	100,0	100,0	100,0	100,0	100,0
5.1. Индивидуальные	1,2	1,8	2,2	2,4	1,7
5.2. Национальные группы хакеров	25,7	20,9	27,2	24,4	9,4
5.3. Международные группы хакеров	56,2	49,6	40,2	37,4	42,6
5.4. Правительственные организации / частные военные корпорации	16,9	27,7	30,4	40	46,3

Источник: авторская разработка.

[12] Актуальные киберугрозы: итоги 2021 года. Аналитический отчет агентства информационной безопасности Positive Research (19.04.2022). [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021/.

[13] Актуальные киберугрозы: итоги 2020 года. Аналитический отчет агентства информационной безопасности Positive Research (28.04.2021). [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/.

[14] Актуальные киберугрозы: итоги 2019 года. Аналитический отчет агентства информационной безопасности Positive Research (18.03.2020). [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019/.

[15] Актуальные киберугрозы – 2017: тренды и прогнозы. Аналитический отчет агентства информационной безопасности Positive Research (06.03.2018). [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2017/.

[16] Сбербанк предсказал рост ущерба экономике России от кибератак на 40 % (21.01.2020). [Электронный ресурс]. URL: https://www.rbc.ru/finances/21/01/2020/5e26e6a79a7947798bc80db7.

[17] «Лаборатория Касперского» оценила потери российского бизнеса от кибератак (21.10.2021). [Электронный ресурс]. URL: https://www.vedomosti.ru/technology/news/2021/10/12/890858-laboratoriya-kasperskogo-otsenila-poteri-rossiiskogo-biznesa-ot-kiberatak.

[18] Рассчитывается как количество успешных тестовых атак, % к общему количеству проведенных пентестов.

Как следует из приведенных в табл. 2 данных, Россия в анализируемом периоде столкнулась не только с растущим количеством организованных кибератак (+1239 ед. к 2017 г., или 205,0 %), но и их структурной концентрацией вокруг финансовых институтов (в среднем на них пришлось 32,0 %), объектов критической инфраструктуры (22,9 %) и государственных учреждений (15,6 %), причем в 2021 г. отмечен явный всплеск атак на критическую инфраструктуру (+6,4 п.п.) и государственные институты (+4,8 п.п.). Конечно, такие доводы являются косвенными аргументами, доказывающими реальность военного характера кибератак, но в них есть ряд различных особенностей от классических хакерских актов: *во-первых*, зафиксированные атаки отличаются очень высоким уровнем организации, жесткой программой действий и дисциплиной участников, характерных больше для силового блока, чем для хактивистов[19]; *во-вторых*, целями атак на госучреждения выступала полная компрометация ИТ-инфраструктуры; кража конфиденциальной информации (почтовых переписок, файлов общего и ограниченного доступа, инфраструктурных и логических схем и т.д.); *в-третьих*, использование в атаках недетектируемого ВПО, легитимных утилит и понимания внутренней логики работы применяемых в органах власти средств защиты информации[20].

Анализируя уровень защищенности отраслей национальной экономики РФ, следует отметить положительное снижение респондентов с критически низкой/низкой оценкой (27,7 % в 2021 г. против 45,9 % в 2020 г.) и одновременным ростом респондентов с оценкой «достаточный уровень защищенности» (40,2 % в 2021 г. против 28,7 % в 2017 г.), вместе с тем публичные данные тематических отчетов (PT Research; SecurityLab) не позволяют увидеть, кому принадлежат такие оценки, а значит, вопрос защищенности критической инфраструктуры и государственных институтов остается открытым.

Переходя к географической структуре совершенных кибератак на цифровое пространство РФ, сразу выделяется тренд увеличения доли международных хакерских группировок (42,6 % по состоянию на конец 2021 г.) и правительственных организаций и частных военных корпораций (46,3 против 16,9 % соответственно). По данным МИД РФ в 2022 г. в связи со специальной военной операцией в Украине в кибератаках против России задействованы 22 хакерские группировки, в том числе из США, Украины и Грузии[21]. Все это свидетельствует не только о росте агрессивности киберсреды, но и постепенном системном разворачивании против национальных интересов России серии военных кибероперaций.

На следующем этапе рассмотрим структуру целей совершаемых кибератак против национальных интересов РФ в 2017–2021 гг. (рис. 1).

---

[19] Кибертерроризм: виды атак, хакеров и их влияния на цели (28.11.2022). [Электронный ресурс]. URL: https://www.securitylab.ru/analytics/534885.php.

[20] Отчет об исследовании серии кибератак на органы государственной власти Российской Федерации (2021). [Электронный ресурс]. URL: https://rt-solar.ru/upload/iblock/53e/Otchet-Solar-JSOC-ob-issledovanii-serii-kiberatak-na-organy-gosudarstvennoy-vlasti-RF-_-web.pdf.

[21] МИД РФ: более 20 хакерских группировок задействованы в операциях против России (09.06.2022). [Электронный ресурс]. URL: https://www.kommersant.ru/doc/5395981.

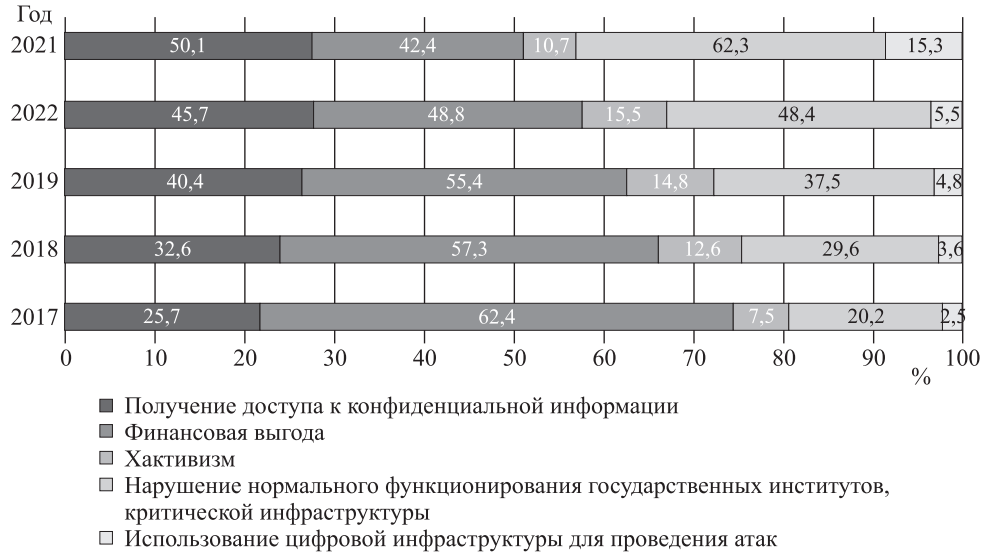

Рис. 1. Структура целей совершаемых кибератак против национальных интересов РФ в 2017–2021 гг., %[12–15, 22]

Источник: авторская разработка

The structure of the goals of cyberattacks against the national interests of the Russian Federation in 2017–2022, %

На основании представленного графика к 2021 г. акцент в кибератаках сконцентрировался на получении доступа к конфиденциальной информации (среднее значение – 38,9 %), финансовой выгоды (53,3 %) и нарушению нормального функционирования государственных институтов, критической инфраструктуры (39,6%), т.е. виден рост заинтересованности в атаках нанесения существенного ущерба не только для неопределенно широкого круга лиц (это отличительная черта хакинга), а именно для дискредитации и нарушения нормального функционирования объектов критической инфраструктуры: по данным «Ростелеком-Солар» за 2021 г. в России было выявлено 300 таргетированных атак[23] на объекты критической информационной инфраструктуры (ЦОДы, серверы портала Госуслуги, Министерства обороны).

В завершении научного исследования рассмотрим структуру расходов государственных регуляторов и уполномоченных институтов информационной безопасности на обеспечение кибербезопасности в 2017–2020 гг.

На рис. 2 показано, как государственные регуляторы в сфере кибербезопасности (Национальный координационный центр по компьютерным инцидентам, Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере) к 2021 г. сместили акцент на сдерживание угроз на внешнем периметре за счет лучшего технического оснащения

[22] Кибербезопасность 2022–2023. Тренды и прогнозы (13.01.2023). [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/.

[23] Крупнейшие кибериниденты и утечки данных в 2021 г. (30.12.2021). [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Threats_Analysis/Biggest-cyber-incidents-and-data-breaches-in-2021.

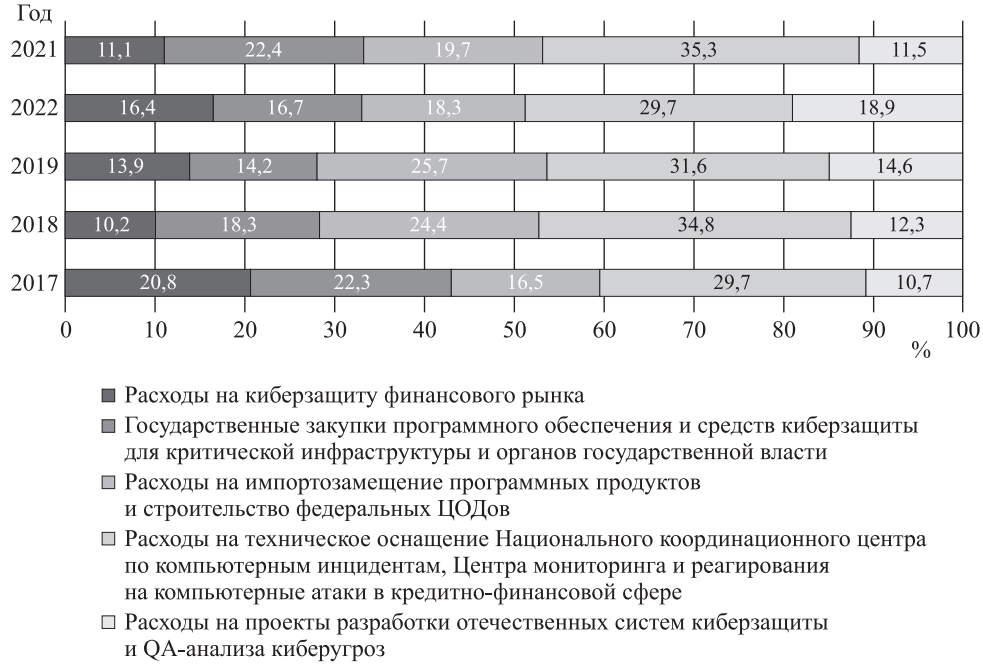

Рис. 2. Структура расходов государственных регуляторов и уполномоченных институтов информационной безопасности на обеспечение кибербезопасности в 2017–2020 гг., % к итогу[24–28]

The structure of expenses of state regulators and authorized information security institutions for ensuring cybersecurity in 2017–2020, % of the total

ядра: так, удельный вес расходов на техническое оснащение Национального координационного центра по компьютерным инцидентам, Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере вырос с 29,7 % в 2017 г. до 35,3 % в 2021 г. Для сравнения расходы на проекты разработки отечественных систем киберзащиты и QA-анализа киберугроз за этот же период времени выросли с 10,7 до 11,5 %. Значительный удельный вес остался за расходами на импортозамещение программных продуктов и строительство федеральных ЦОДов – среднее значение составило 20,9 %.

[24] Весь кибербез за один час. Итоги 2021 года и прогнозы на 2022 в области кибербезопасности по версии Positive Technologies (20.01.2022). [Электронный ресурс]. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Positive_Technologies_Whitepaper_ves-kiberbez-za-chas_20_01_2022.pdf.

[25] Информационная безопасность на практике. Итоги 2018 г., перспективы 2019 г. (2021). [Электронный ресурс]. URL: https://www.securitycode.ru/upload/iblock/119/Info_Security_in_practice_2019.pdf.

[26] Компромисс бюджета и информационной безопасности (26.12.2018). [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/regional-information-security-2018/ (дата обращения: 27.12.2022, доступ: свободный).

[27] Сколько стоит информационная безопасность (18.12.2017). [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/is-cost-2017/.

[28] Обзор операций, совершенных без согласия клиентов финансовых организаций в 2021 г. (11.04.2022). [Электронный ресурс]. URL: https://cbr.ru/analytics/ib/operations_survey_2021/.

Обсуждение. Таким образом, в России сформирована и продолжает развиваться *централизованная модель управления информационной безопасностью в цифровой экономике*, что укладывается в уже отлаженную вертикально интегрированную модель государственного управления, однако важной чертой ее эффективного функционирования является необходимость глубокого проникновения в информационное окружение каждого из граждан, бизнесов и некоммерческих организаций. Только при таком условии обеспечивается возможность проактивного реагирования на внутренние и внешние киберугрозы и атаки, однако это в свою очередь порождает многочисленные опасения по поводу формирования в России так называемого «цифрового гетто», т.е. полного подчинения сферы ИКТ интересам политической элиты и существенного ограничения свобод граждан в целом, что является фейком в своей сути, но тем не менее приводит к паническим настроениям в обществе[29] и еще сильнее усиливает нестабильность информационного периметра государства и повышает риски ослабления цифрового суверенитета.

Простого решения данного вопроса нет, так как он требует перекраивания механизма управления социально-экономическими процессами в пользу повышения цифровой гигиены и культуры поведения граждан в информационном пространстве, включение в образовательные курсы, начиная со школы занятия в области кибербезопасности и разъяснения опасностей перерастания организованных кибератак в полноценную кибервойну.

Второй существенной проблемой является *нарастание разрыва в обеспечении киберзащиты в наиболее привлекательных для кибератак сферах и отраслях*: кредитно-финансовой, здравоохранении, государственном управлении, объектах энергетической и иной критической инфраструктуры. Так, например, в банковском секторе удельный вес ТОП-10 крупнейших банков в совокупных расходах финансово-кредитного сектора на кибербезопасность составляет по итогам III квартала 2022 г. по разным оценкам от 48,7 до 54,1 % (зависит от политики конфиденциальности предоставления данных)[30], т.е. имеем мощное защищенное ядро на финансовом рынке, в то время как более 36,0 % представителей топ-менеджмента банков более низкого уровня заявили об отсутствии в составе их оргструктуры самостоятельной команды специалистов в области информационной безопасности. Такое положение дел в перспективе будет приводить к массовому отзыву лицензий, перевод на основании плохого риск-профиля будет вытеснять такие банки на периферию рынка и потерю клиентской базы[31].

Атаки на медучреждения связаны с развитием телемедицины и развития практики виртуального обмена информацией между пациентом и врачом, что является интересным объектом для атак прежде всего коммерческого характера (продажа, деанонимизация данных о болезнях). Согласно

[29] Большой брат: чего добивается движение за визуальную приватность (01.10.2020). [Электронный ресурс]. URL: https://trends.rbc.ru/trends/futurology/5f75e6349a7947957f334e71.

[30] Аналитический отчет Positive Technologies 2022. [Электронный ресурс]. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/positive-research-2022-rus.pdf.

[31] ЦБ введет новое наказание для банков за плохую защиту от кибератак (12.09.2019). [Электронный ресурс]. URL: https://www.rbc.ru/finances/12/09/2019/5d7a444b9a79473704c454a2.

данным отчета PT Research из зафиксированных 227 атак на сферу здравоохранения, 192 из них связаны с невозможностью своевременного обновления архитектуры программного обеспечения из-за введенных санкций на покупку лицензий для профильного оборудования[32].

Ввиду доминирования государственного сектора в сфере здравоохранения автором высказано предположение о необходимости развития практики путем внесения поправок в Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья» от 29.07.2017 N 242-ФЗ[33] через развитие платформы «Здоровье», представляющее создание сети региональных аналитических платформ для комплексной автоматизации бизнес-процессов оказания медицинской помощи, обеспеченное новейшими технологиями защиты, включая блокчейн.

Третьей сложной проблемой обеспечения эффективной защиты от организованных кибератак национальной экономики России является *массовая релокация опытных IT-специалистов и множественность введенных санкций против сектора информационно-компьютерных технологий*: по итогам трех кварталов 2022 г. число санкций превысило 500 ед., в том числе сокращение трансферта технологий и совместных R&D проектов – более 200, сокращение / запрет на инвестиции в российский сектор ИКТ (включая венчурные фонды) – более 187 ед. Количество специалистов-релокантов сектора ИКТ за этот же интервал времени составило более 100 000 чел., число компаний-релокантов – более 120 ед.[34–36]

Для преодоления дефицита государственным регулятором принимается комплекс мер по введению финансовых стимулов и налоговых послаблений для IT-компаний для сохранения их деловой активности и присутствиям на российском рынке: освобождение от налогообложения НДС операций по передаче исключительных прав на программы, базы данных, включенных в единый реестр российского ПО (п. 7 письма ФНС от 18.12.2020 № СД-4-3/20902[37]): программные продукты для объектов критической инфраструктуры ИКТ-сферы, государственный заказ в рамках импортозамещения; ГК «РВК» и его партнеры: РФРИТ, фонд «Сколково» и ФРИИ[38]

---

[32] Атаки на здоровье: какие кибервызовы стоят перед современной медициной (2021). [Электронный ресурс]. URL: https://trends.rbc.ru/trends/industry/637f2a909a794747ebe66926.

[33] «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья» от 29.07.2017 N 242-ФЗ. [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_221184/.

[34] Дефицит ИТ-мозгов: как Россия решает проблему кадрового голода в отрасли (28/07/2022). [Электронный ресурс]. URL: https://www.rbc.ru/economics/28/07/2022/62e12c929a794747597da279.

[35] Рынок труда в России (ИТ и телеком) (01/11/2022). [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Рынок_труда_в_России_(ИТ_и_телеком).

[36] Период IT-распада: как спасти российскую отрасль кибербезопасности (27.12.2022). [Электронный ресурс]. URL: https://www.ng.ru/economics/2022-11-02/100_215701112022.html.

[37] О налоговом маневре в IT-отрасли: Федеральная налоговая служба: Письмо № СД-4-3/20902 от 18.12.2020 (01.10.2021). [Электронный ресурс]. URL: https://www.klerk.ru/doc/519824/.

[38] Льготы для ИТ-компаний в 2022 году: основные меры поддержки и как их получить (18.05.2022). [Электронный ресурс]. URL: https://www.it-world.ru/it-news/state/184625.html.

предлагают широкий круг грантов в размере 20–500 млн руб. на разработку российских аналогов программных продуктов в сфере информационной безопасности для критической инфраструктуры и госучреждений; проведение национальной аккредитации ИКТ-компаний для более тщательного контроля за их деятельностью[39].

Заключение. Подводя итог научного исследования, следует отметить следующее: цифровая война является «ближайшим родственником» к гибридной войне, но отличается от нее более высоким уровнем самоорганизации и сущностно-функциональной автономностью, и удаленностью от места протекания, так как может вестись самостоятельно без прибегания к использованию вооруженных сил. В РФ в отличие от зарубежной практики в национальном законодательстве отсутствует закрепленный термин «цифровая война», что усложняет анализ произошедших кибератак на предмет участия в них правительств и военных институтов стран-противников. В границах хронологического периода анализа был установлен факт структурной концентрации организованных кибератак вокруг финансовых институтов, объектов критической инфраструктуры и государственных учреждений, причем в 2021 г. отмечен явный всплеск атак на критическую инфраструктуру и государственные институты.

На сегодняшний день в России сформирована и продолжает развиваться *централизованная модель управления информационной безопасностью в цифровой экономике*, что укладывается в уже отлаженную вертикально интегрированную модель государственного управления, однако важной чертой ее эффективного функционирования является необходимость глубокого проникновения в информационное окружение каждого из граждан, бизнесов и некоммерческих организаций, а это приводит к паническим настроениям в обществе и еще сильнее усиливает нестабильность информационного периметра государства и повышает риски ослабления цифрового суверенитета.

Список источников

1. *Балаклеец Н.А*. Пространственный аспект современных войн: от традиционной войны к кибервойне // Социодинамика. 2021. № 4. С. 136–148. DOI: 10.25136/2409-7144.2021.4.32652
2. *Бегларян М.Е., Войтова-Долгих Я.Н., Одинцов С.А*. Исторические аспекты понятий «киберпреступление» и «кибертерроризм» в законодательстве: проблемы трактования // Вестник Краснодарского университета МВД России. 2020. № 4. С. 11–16.
3. *Глазьев С.Ю*. Украинская катастрофа: от американской агрессии к мировой войне? («Коллекция Изборского клуба»). М.: Книжный мир, 2015. 352 с.
4. *Дугин А.Г*. Русская война / под ред. В.М. Коровина. М.: ООО «ТД Алгоритм», 2015. С. 147.
5. *Животова О.Н*. Война как высшая форма проявления политического конфликта // Актуальные исследования. 2021. № 31 (58). С. 10–12.

[39] Прогноз развития рынка кибербезопасности в Российской Федерации на 2022–2026 годы (2022). [Электронный ресурс]. URL: https://www.csr.ru/upload/iblock/13f/ufleu9rg5zc3ldu66srqt3a89j0mrve5.pdf.

6. *Тиханычев О.В*. Гибридные войны: новое слово в военном искусстве или хорошо забытое старое? // Вопросы безопасности. 2020. № 1. С. 30–43. DOI: 10.25136/2409-7543.2020.1.30256
7. *Уэбстер Ф*. Теории информационного общества. М.: Аспект пресс, 2004. 400 с.
8. *Хайек Ф*. Дорога к рабству. М.: Изд-во АСТ, 2017. 320 с.
9. *Хеджес К*. Шелдон Волин и перевернутый тоталитаризм // Социологические исследования. 2021. № 6. С. 147–153.
10. *Чернышенко Н.А*. Кибервойна: теория и практика // Научные работы. Политология. 2015. Т. 248. С. 37–42.
11. *Cristiano F*. From Simulations to Simulacra of War: Game Scenarios in Cyberwar Exercises // Journal of War and Culture Studies. 2018. Vol. 11, no. 1. P. 22–37. DOI: 10.1080/17526272.2017.1416761
12. *Cronin A.K*. Behind the Curve: Globalization and International Terrorism. Essential Readings in World Politics / Ed. by K.A. Mingst, J.L. Snyder. N. Y.: W. W. Norton & Company, 2004. P. 367–381.
13. *Evans G., Newnham J*. Dictionary of International Relations. L.: Penguin Reference, 1998. 597 p.
14. *Gibbs J.P*. Conceptualization of Terrorism // American Sociological Review. 1989. Vol. 54, no. 3. P. 329–340.
15. *Harknett R.J., Smeets M*. Cyber campaigns and strategic outcomes // Journal of Strategic Studies. 2020. Vol. 4. P. 36–42. DOI: 10.1080/01402390.2020.1732354
16. *Holt T.J., Freilich J.D., Chermak S.M*. Exploring the Subculture of Ideologically Motivated Cyber-Attackers // Journal of Contemporary Criminal Justice. 2017. Vol. 33, no. 3. P. 212–233. DOI: 10.1177/1043986217699100

References

1. Balakleec N.A. Prostranstvennyj aspekt sovremennyh vojn: ot tradicionnoj vojny k kibervojne [Spatial aspect of modern wars: from traditional war to cyber war], *Sociodinamika* [*Sociodynamics*], 2021, no. 4, pp. 136–148. DOI: 10.25136/2409-7144.2021.4.32652
2. Beglarjan M.E., Vojtova-Dolgih Ja.N., Odincov S.A. Istoricheskie aspekty ponjatij «kiberprestuplenie» i «kiberterrorizm» v zakonodatel'stve: problemy traktovanija [Historical aspects of the concepts of "cybercrime" and "cyberterrorism" in legislation: problems of interpretation], *Vestnik Krasnodarskogo universiteta MVD Rossii* [*Vestnik of the Krasnodar University of the Ministry of Internal Affairs of Russia*], 2020, no. 4, pp. 11–16.
3. Glaz'ev S.Ju. Ukrainskaja katastrofa: ot amerikanskoj agressii k mirovoj vojne? [Ukrainian catastrophe: from American aggression to world war?] («Kollekcija Izborskogo kluba»). Moscow, Knizhnyj mir, 2015. 352 p.
4. Dugin A.G. Russkaja vojna [Russian war]. Pod red. V.M. Korovina. Moscow, OOO «TD Algoritm», 2015. P. 147.
5. Zhivotova O.N. Vojna kak vysshaja forma projavlenija politicheskogo konflikta [War as the highest form of manifestation of political conflict], *Aktual'nye issledovanija* [*Actual research*], 2021, no. 31 (58), pp. 10–12.
6. Tihanychev O.V. Gibridnye vojny: novoe slovo v voennom iskusstve ili horosho zabytoe staroe? [Hybrid wars: a new word in military art or a well-forgotten old one?], *Voprosy bezopasnosti* [*Security questions*], 2020, no. 1, pp. 30–43. DOI: 10.25136/2409-7543.2020.1.30256
7. Ujebster F. Teorii informacionnogo obshhestva [Theories of the information society]. Moscow, Aspekt press, 2004. 400 p.
8. Hajek F. Doroga k rabstvu [Road to slavery]. Moscow, Izd-vo AST, 2017. 320 p.

9. Hedzhes K. Sheldon Volin i perevernutyj totalitarizm [Sheldon Wolin and inverted totalitarianism], *Sociologicheskie issledovanija* [*Sociological research*], 2021, no. 6, pp. 147–153.
10. Chernyshenko N.A. Kibervojna: teorija i praktika [Cyber warfare: theory and practice], *Nauchnye raboty. Politologija* [*Scientific works. Political science*], 2015, vol. 248, pp. 37–42.
11. Cristiano F. From Simulations to Simulacra of War: Game Scenarios in Cyberwar Exercises. Journal of War and Culture Studies, 2018, vol. 11, no. 1, pp. 22–37. DOI: 10.1080/17526272.2017.1416761
12. Cronin A.K. Behind the Curve: Globalization and International Terrorism. Essential Readings in World Politics / Ed. by K.A. Mingst, J.L. Snyder. N. Y.: W. W. Norton & Company, 2004. P. 367–381.
13. Evans G., Newnham J. Dictionary of International Relations. L.: Penguin Reference, 1998. 597 p.
14. Gibbs J.P. Conceptualization of Terrorism. *American Sociological Review*, 1989, vol. 54, no. 3, pp. 329–340.
15. Harknett R.J., Smeets M. Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*, 2020, vol. 4, pp. 36–42. DOI: 10.1080/01402390.2020.1732354
16. Holt T.J., Freilich J.D., Chermak S.M. Exploring the Subculture of Ideologically Motivated Cyber-Attackers. *Journal of Contemporary Criminal Justice*, 2017, vol. 33, no. 3, pp. 212–233. DOI: 10.1177/1043986217699100

Сведения об авторе:

А.С. Ермаков – аспирант, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, ООО «Инсейлс Рус», Москва, Российская Федерация.

Information about the author:

A.S. Ermakov – Graduate student, Russian Presidential Academy of National Economy and Public Administration, Insales Rus LLC, Moscow, Russian Federation.

Статья поступила в редакцию	*11.01.2023*	*The article was submitted*	*11.01.2023*
Одобрена после рецензирования	*02.02.2023*	*Approved after reviewing*	*02.02.2023*
Принята к публикации	*16.02.2023*	*Accepted for publication*	*16.02.2023*