УДК 342.5-042.4:004
DOI 10.20339/AM.07-23.019

Д.Н. Иванов,
канд. ист. наук
доцент кафедры международного предпринимательства (кафедра 83)
Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП)
SPIN-код: 9787-0485
ORCID 0000-0002-8915-6014
e-mail: ivanov_d_n@inbox.ru

ВЕБ-СВЕРХДЕРЖАВА

В условиях интенсивного развития информационных технологий и постепенного перемещения различных функций государства в онлайн (вспомним тот же портал «Госуслуги»), а также многочисленных виртуальных сред, в которых реальные люди через свои аватары взаимодействуют с аватарами других людей, рано или поздно должны были появиться проекты, стремящиеся создать из подобной виртуальной реальности некую структуру с признаками государства. Первой более-менее значимой попыткой на этом фоне было создание «блокчейн-государства "Decenturion"», которое на сегодняшний день прекратило свое существование и рассматривается многими уже не как визионерская попытка создания нового субъекта права, а как несколько специфическая, но хорошо известная «финансовая пирамида». Тем не менее следует ожидать, что в дальнейшем мы увидим еще некоторые попытки создания квазигосударственных образований в виртуальном мире, и некоторые из них, вероятно, смогут обрести и определенный вес в мире реальном. В статье рассматриваются критерии, позволяющие отнести государство к числу сверхдержав и принципиальная возможность появления в XXI веке в интернете образования, идентифицирующего себя как государство и соответствующего критериям сверхдержавы.

Ключевые слова: *веб-сверхдержава, интернет-государство, онлайн-государство, Децентурион.*

WEB SUPERPOWER

Dmitrii N. Ivanov, Cand. Sci (History), Associate Professor of the Department of International Entrepreneurship (Department 83) at Saint-Petersburg State University of Aerospace Instrumentation, SPIN-code: 9787-0485, ORCID: 0000-0002-8915-6014, e-mail: *ivanov_d_n@inbox.ru*

In the context of the intensive development of information technologies and the gradual transfer of various functions of the state online (remember the same portal "Gosuslugi"), as well as numerous virtual environments in which real people interact through their avatars with the avatars of other people, sooner or later projects should appear, seeking to create from such a virtual reality a certain structure with the features of the state. The first more or less significant attempt against this background was the creation of the "decenturion blockchain state", which has ceased to exist today and is considered by many no longer as a visionary attempt to create a new subject of law, but as a somewhat specific, but well-known "financial pyramid". However, we should expect that in the future we will see some more attempts to create quasi-state formations in the virtual world, some of which will probably be able to gain some weight in the real world. The article discusses the criteria that make it possible to attribute the state to the number of superpowers and the fundamental possibility of the appearance in the 21st century on the Internet of an education that identifies itself as a state and meets the criteria of a superpower.

Keywords: *web superpower, internet state, online state, Decenturion.*

Введение

Может ли существовать великая держава или даже сверхдержава, не имеющая территории в привычном понимании этого слова? Площадь которой — не квадратные километры, а байты. Население — не люди, а аватары. Экономика… А вот экономика, пожалуй, выглядит в реалиях современной цифровизации более привычной: производство цифрового продукта, блокчейн-технологии, инвестиции в стартапы…

Для начала разделим два понятия: государство и великая держава.

Сам термин «великая держава» вошел в широкое употребление благодаря статье Леопольда фон Ранке «Великие державы» во втором номере Историко-политического журнала за 1833 г. Он называет пять «великих держав»: Австрия, Великобритания, Пруссия, Россия и Франция [1]. Аналогично широкое употребление приобрел и термин «сверхдержава» благодаря книге У.Т.Р. Фокса «Сверхдержавы: Соединенные Штаты, Соединенное Королевство и Советский Союз — их ответственность за мир», опубликованной в 1944 г. [2]. Таким образом, к середине XX в. число действительно влиятельных государств в мировом масштабе сократилось до трех, а немного позднее — и вовсе до двух. Это отразилось и в терминах, которые использовали авторы работ.

По большому счету, наиболее очевидный критерий отнесения страны к числу «великих» или «сверхдержав» — это вооруженные силы. В качестве распространенности подобного подхода можно сослаться на знаменитый вопрос И.В. Сталина, адресованный У. Черчиллю во время их встречи в Москве в октябре 1944 г.: «А сколько дивизий у папы римского?» [3]. Чем больше армия и/или флот, тем больше у страны возможностей влиять на политику других государств в мировом масштабе. Эта логика (с поправкой на техническое оснащение вооруженных сил и их возможность действовать далеко за пределами приграничных территорий собственной страны) в целом работает и в сегодняшних реалиях.

Но постепенно такой подход устаревает. И речь идет не только о широком применении роботизированных систем

вооружения (включая постоянно упоминаемые в наши дни военные дроны).

До относительно недавнего времени мир был полностью «аналоговым». Иными словами, нанесение реального, «физического» урона требовало непосредственно «физического» контакта: чтобы вывести из строя промышленное предприятие или его часть, требовалось либо устроить диверсию непосредственно на территории предприятия, либо нанести по нему удар с помощью артиллерии, бомб или ракет. То же самое касалось практически любого объекта инфраструктуры на любом уровне. Даже банальное прослушивание телефона требовало физического подключения к телефонному аппарату или к кабелю. Эти методы остаются достаточно действенными и в наши дни.

Однако сегодня далеко не обязательно находиться рядом с объектом воздействия, чтобы добиться поставленной цели: разговоры по тому же мобильному телефону достаточно легко прослушиваются с использованием оборудования чуть выше бюджетного уровня [4; 5]. В эпоху цифровизации и интернета холодильник скоро сможет самостоятельно проверить срок годности хранящихся в нем продуктов и заказать доставку испортившихся [6]. Элементами «умного дома» — от телевизора до электророзетки — сегодня уже никого не удивишь [7]. Но быт — далеко не первый рубеж повсеместной цифровизации. Куда раньше она внедрилась в рабочие процессы: управление станками и оборудованием, дистанционная диагностика, связь… Для нанесения ощутимого экономического ущерба вовсе не обязательно находиться рядом с объектом атаки. Вирус, попавший в компьютеры завода, отвечающие за работу оборудования (как производственного, так и составляющего инфраструктуру самого предприятия), способен нанести ущерб, сопоставимый с попаданием ракеты. Самым известным подобным примером может служить атака израильских и американских спецслужб на иранский завод в Натанзе, занимавшийся обогащением урана, — успешно внедренный «червь» смог нанести физический ущерб всем урановым центрифугам завода и как минимум приостановить иранскую ядерную программу [8; 9].

Нельзя сказать, чтобы в сегодняшних условиях численность вооруженных сил не имела значения. Однако удар по цифровой инфраструктуре может парализовать едва ли не все процессы в государстве — особенно если учесть, что часть документооборота сегодня существует **только** в электронном виде. Например, свидетельство о праве собственности на недвижимость в Российской Федерации с 2016 г. выдается только в электронном виде [10], и в случае повреждения этих данных восстановить права собственности будет крайне сложно: нет документа на защищенной бумаге с индивидуальным номером и книги учета выдачи таких документов, где номер зафиксирован. Поражение цифровой инфраструктуры (в том числе прекращение доступа в интернет) вполне может остановить даже внутригородские пассажирские перевозки (кондукторов в общественном транспорте в крупных городах становится все меньше, нередко поднимается вопрос о полном отказе от этой категории транспортных служащих [11]) и розничную торговлю (для работы платежных терминалов на кассах необходимо интернет-соединение). Собственно, мини-демонстрация возможного удара по безналичной оплате товаров и услуг произошла сперва в 2014 г., когда платежные системы Visa и MasterCard прекратили обслуживание ряда банков, оказавшихся под санкциями США [12], а затем в 2022, когда возникли проблемы с оплатой товаров через ApplePay и GooglePay [13].

Поэтому можно допустить, что сегодня возможности действий в цифровом мире вполне сопоставимы по своей эффективности с возможностями действий в мире физическом и, более того, происходящее в цифровом мире влияет на происходящее в «реальном» мире (причем обратное влияние, скорее всего, существенно скромнее).

Отсюда встает вопрос: допустимо ли говорить о принципиальной возможности возникновения цифровой сверхдержавы? Причем под цифровой сверхдержавой будет подразумеваться не некое реальное государство, существующее в реальном мире — неважно, это международно признанное, или непризнанное (как Приднестровская Молдавская Республика), или «виртуальное», как часто называются небольшие территории, провозглашающие себя суверенными государствами (такие как Силэнд), — а объединение, существующее исключительно в интернете и при этом позиционирующее себя как государство. В дальнейшем будем именовать такое образование веб-государством, чтобы не путать его с виртуальным государством [14], цифровым государством [15] и другими схожими терминами, поскольку эти понятия достаточно активно используются в публицистике и научной литературе, однако нередко обозначают цифровую часть реального государства (например, онлайн-сервисы правительственных учреждений) или образования, занимающие вполне конкретную территорию, но не получившие международного признания и/или имеющие не бесспорный суверенитет над занимаемой территорией [16].

Основная часть

Основные составляющие веб-государства

Насколько корректно говорить о веб-государстве как о собственно государстве — предмет отдельного исследования. В данном случае важно другое: может ли такое веб-государство стать сверхдержавой (веб-сверхдержавой)? Если оставить в стороне вопрос о формально-юридическом признании цифрового образования государством и исключить фактор наличия вооруженных сил (по крайней мере в привычном значении этого слова — родов войск, таких как общевойсковые части, бронетанковые войска, военно-воздушные силы и др.) и оставить только приобретение значимого политического влияния в мировом масштабе — то, безусловно, может.

Допустимо постулировать, что политическое влияние складывается из трех основных компонентов:

- морального авторитета;
- экономической мощи;
- возможностей вооруженных сил.

Сложнее всего оценить моральный авторитет и тем более отделить его от экономических и военных возможностей государства — особенно если оценивается потенциальный авторитет структуры, которая еще только делает свои первые шаги (например, веб-государство Децентурион, возникшее в 2018 г., признавалось некоторыми исследователями практической демонстрацией государственно-правовых возможностей блокчейна [17]). Любые предположения здесь будут носить спекулятивный характер.

В чем основное преимущество веб-государства? В общедоступности (стать его гражданином куда проще, нежели любого другого государства, если не говорить о гражданстве по рождению), максимально прозрачной и демократичной системе управления, в ощущении причастности к чему-то новому, передовому, прогрессивному, возможно, даже визионерскому. Безусловно, сама идея такого государства обеспечит ему определенную группу сочувствующих во всем мире, в том числе среди представителей IT-сообщества и близких к нему структур. Скорее всего, эта группа не будет многочисленной (для обычного человека речь идет о слишком уж экзотическом опыте), но может оказаться достаточно влиятельной благодаря таким людям как Стив Джобс, Илон Маск и Билл Гейтс. IT-индустрия стала в том числе достаточно публичной — к мнению наиболее медийных ее представителей прислушиваются даже люди, далекие от мира единиц и нулей. К тому же веб-государство сможет продавать образ своего рода Утопии — государства с максимальной децентрализацией и минимальным регулированием; образ общества, предельно приближенного к анархическому в классическом понимании этого термина (как у Прудона). А этот «товар» найдет куда более обширный отклик как минимум у молодежной и, возможно, даже подростковой аудитории.

Экономические возможности также оценить непросто: опять же, слишком небольшой отрезок времени прошел для того, чтобы можно было говорить о серьезных цифрах, равно как и о самой перспективе существования Децентуриона (на данный момент проект, похоже, прекратил свое существование [18]) или подобных ему образований. Несмотря на формальную открытость, кроме декларации о передаче 100% ВВП Децентуриона резидентам государства, найти точные данные об объеме ВВП Децентуриона не удалось. Тем не менее сама модель инвестиций в стартапы (во многом похожая на работу краудфандинговых платформ) при определенных условиях может оказаться работоспособной.

Другим возможным направлением экономики веб-государств может быть объединение людей для создания интеллектуальной продукции, если в подобном веб-государстве будут эффективные инструменты коммуникации (возможно, с применением технологий виртуальной реальности). В результате может быть создано все что угодно — от художественной литературы до чертежей завода, от простенького таймкиллера для смартфонов до программ – симуляторов работы научных инструментов (например, БАКа).

А вот военные возможности… Тут все намного интереснее. С одной стороны, классических вооруженных сил у веб-государства быть не может. С другой — кибервойска анонсированы рядом стран мира (в США об их создании впервые официально заявили в 2013 г. [19], а тройку лидеров в этой сфере составляют США, Китай и Великобритания [20]). Веб-государство вполне может располагать собственной киберармией. Мировая практика показывает, что для эффективной DDoS-атаки хватает и одного человека (в 2000 г. школьник Майк Калс «уложил» ряд сайтов, включая Yahoo, Dell, Amazon [21; 22]). Был и опыт атак на целые страны: на Эстонию в 2007 г. [23] и Беларусь в 2020 г. [24], хотя источник атак в этих случаях остался неизвестен широкой общественности. То есть небольшая по численности группа хакеров вполне может нанести ощутимый вред даже государственной инфраструктуре. А значит, для веб-государства создание киберармии — выполнимая задача.

Разумеется, возникает проблема локализации. Для ряда процессов (то же хранение информации) вопрос физической территории не принципиален: как правило, информация дублируется и распределяется между несколькими местами хранения, так что выход из строя одного-двух серверов заметного ущерба самой информации не наносит. Но кибервойска состоят из реальных людей, проживающих на территории вполне реальных стран (если не выбрать местом постоянного проживания, допустим, судно, находящееся в нейтральных водах). Действия в интересах третьих стран, включая и веб-государства, направленные на нанесение ущерба физическим, юридическим лицам (в том числе ущерба виртуальному имуществу — тем же сайтам, например) или даже целым странам в подавляющем большинстве случаев вызовут недовольство местных правоохранительных органов. Поэтому, в отличие от большинства «граждан» такого веб-государства, для солдат кибервойск веб-государства выбор места физического проживания будет иметь принципиальное значение. А это снижает степень свободы, которая является, пожалуй, главной отличительной чертой веб-государства в сравнении с государством физическим. Список пригодных для проживания солдат веб-государства стран будет весьма скромным: требуется высокоскоростной и стабильный интернет, нейтральный статус самого государства, отсутствие договоров об экстрадиции с большинством стран мира, лояльность местных органов власти по отношению к тем, кого во многих странах мира идентифицировали бы как кибертеррористов, и серьезные препятствия для свободной деятельности на территории, избран-

ной киберсолдатом веб-государства для проживания, спецслужб стран — потенциальных противников веб-государства. Пожалуй, под все эти требования не подойдет ни одно государство мира. С оговорками могут рассматриваться такие страны, как Соломоновы Острова, Турецкая Республика Северного Кипра или Сахарская Арабская Демократическая Республика.

Тем не менее можно допустить, что веб-государство при определенных условиях может приобрести моральный авторитет (особенно при грамотно организованной пропагандистской компании — чем веб-государство хуже Греты Тунберг?), экономические возможности и даже стать обладателем армии. В теории, если все три показателя достигнут значений, сопоставимых по возможностям с аналогичными показателями ведущих стран мира (таких как США, Китай, Германия), можно будет говорить о веб-сверхдержаве.

Реалистичность веб-сверхдержавы

Значит ли это, что веб-сверхдержава действительно возможна?

С чисто технической точки зрения — да. Но есть одно существенное обстоятельство: международные процессы часто стремительны и требуют от активных участников, претендующих на роль своего рода рулевого в общемировом масштабе, столь же незамедлительной реакции. Такую реакцию могут показать хорошо организованные централизованные государства, где ключевые решения может принимать фактически один человек. В большей или меньшей мере такая возможность реализована почти во всех современных государствах. Этот принцип вполне может быть положен в основу существующего в веб-пространстве государства, но такое образование будет отличаться от обычного государства разве что отсутствием физической территории: будет ярко выраженное деление на элиту и плебс. Это как раз то, от чего многие и стремятся уйти в онлайн. Едва ли веб-государство, созданное по такому принципу, станет популярным. Не случайно многократно упомянутый Децентурион позиционирует себя как государство с прямой демократией. Фактически это означает, что любое решение требует голосования всех граждан государства и будет принято в таком варианте, за который проголосует большинство (т.е. речь идет о проведении референдума). При решении рутинных задач, не требующих быстрого принятия решений, это вполне допустимый вариант выбора способа действий. Но в экстремальных условиях (допустим, военной угрозы: применительно к веб-государству это может означать попытку хакерской атаки на компьютеры, содержащие информацию о веб-государстве) такой механизм становится крайне неэффективным. Он не только не позволяет быстро принимать решения, но и не позволяет эффективно заставить часть граждан веб-государства, не согласившуюся с мнением большинства, действовать в соответствии с одобренной на голосовании схемой. Не случайно в современном мире, как из-за вышеприведенных особенностей, так и из-за чисто технической сложности организации референдума, прямая демократия практически не встречается и в наибольшей мере представлена в Швейцарии.

Вопрос о принципиальной возможности появления веб-сверхдержавы зависит от того, удастся ли кому-нибудь либо создать централизованное веб-государство с четкой вертикалью управления, достаточно популярное, чтобы при этом обрести и моральный авторитет, и развитую экономику, и кибер-армию, либо создать веб-государство с прямой демократией, способное быстро реагировать на вызовы современности. В текущих условиях оба сценария кажутся маловероятными, но не нереальными, а значит, веб-сверх-держава в теории возможна.

Литература

1. *Ranke L. von.* Die großen Mächte. Leipzig: New herausgegeben, 2012. 61 s. [Электронный ресурс] // Project Gutenberg [сайт]. [2012]. URL: https://gutenberg.org/files/39669/39669-h/39669-h.htm (дата обращения: 19.03.2023).

2. *Fox William T.R.* The Super-Powers: The United States, Britain, and the Soviet Union — Their Responsibility for Peace. N-Y, 1944 [Электронный ресурс] // Cambridge University Press [сайт]. [2013]. URL: https://www.cambridge.org/core/journals/american-political-science-review/article/abs/superpowers-the-united-states-britain-and-the-soviet-uniontheir-responsibility-for-peace-by-william-t-r-fox-new-york-harcourt-brace-and-company-1944-pp-162-200-the-great-decision-by-james-t-shotwell-new-york-the-macmillan-company-1944-pp-234-300/62275F7F5673D641D4FCAAAC069A5BCA (дата обращения: 19.03.2023).

3. *Бережков В.М.* Как я стал переводчиком Сталина. М.: ДЭМ, 1993. 400 с. URL: http://militera.lib.ru/memo/russian/berezhkov_vm/06.html (дата обращения: 19.03.2023).

4. *Сноу Д.* Прослушивают всех: взлом GSM-сетей из эфира [Электронный ресурс] // Kaspersky daily: [сайт]. [2016]. URL: https://www.kaspersky.ru/blog/gsm-hijacking/11375/ (дата обращения: 19.03.2023).

5. *Минин П.Е., Самойлов А.С., Кузин А.А.* Уязвимости канала данных Bluetooth для прослушивания злоумышленниками // Безопасность информационных технологий. 2012. № 25. С. 50–53.

References

1. *Ranke, L., von.* Die großen Mächte. Leipzig: New herausgegeben, 2012. 61 s. // Project Gutenberg [website]. [2012]. URL: https:// gutenberg.org/files/39669/39669-h/39669-h.htm (accessed on: 19.03.2023).

2. *Fox, William T.R.* The Super-Powers: The United States, Britain, and the Soviet Union — Their Responsibility for Peace. N-Y, 1944 [Electronic resource] // Cambridge University Press [site]. [2013]. URL: https://www.cambridge.org/core/journals/american-political-science-review/article/abs/superpowers-the-united-states-britain-and-the-soviet-uniontheir-responsibility-for-peace-by-william-t-r-fox-new-york-harcourt-brace-and-company-1944-pp-162-200-the-great-decision-by-james-t-shotwell-new-york-the-macmillan-company-1944-pp-234-300/62275F7F5673D641D4FCAAAC069A5BCA (accessed on: 19.03.2023).

3. *Berezhkov, .M.* How I became Stalin's translator. Moscow: DAM, 1993. 400 p. URL: http://militera.lib.ru/memo/russian/berezhkov_vm/06.html (accessed on: 19.03.2023). (In Rus.)

4. *Snou, D.* Listening to everyone: hacking GSM networks from the airwaves [Electronic resource] // Kaspersky daily [web-site]. [2016]. URL: https://www.kaspersky.ru/blog/gsm-hijacking/11375/ (accessed on: 19.03.2023). (In Rus.)

5. *Minin, P.E., Samojlov, A.S., Kuzin, A.A.* Bluetooth data channel vulnerabilities for intruders to eavesdrop. Bezopasnost' informacionnykh tekhnologii. 2012. 25: 50–53. (In Rus.)

6. *Шевченко М.* Amazon создает умный холодильник, который будет следить за своим содержимым и самостоятельно заказывать продукты [Электронный ресурс] // 3DNews: [сайт]. [2021]. URL: https://3dnews.ru/1050640/amazon-sozdayot-umniy-holodilnik-kotoriy-budet-sledit-za-svoim-sodergimim-i-samostoyatelno-zakazivat-produkti (дата обращения: 19.03.2023).

7. *Zainal Al N.* The architecture of smart internet of things // T-COM. 2021. #8. P. 58–61.

8. *Ромашкина Н.П., Махукова А.В.* Компьютерная вредоносная атака на ядерную программу Ирана // Информационные войны. 2013. № 4 (28). С. 88–98.

9. Самые громкие кибер-атаки на критические инфраструктуры [Электронный ресурс] // Хабр: [сайт]. [2016]. URL: https://habr.com/ru/company/panda/blog/316500/ (дата обращения: 19.03.2023).

10. Свидетельство о праве собственности на недвижимость с 15 июля отменено // Управа района Северное Измайлово города Москвы [сайт]. [2016]. URL: https://sevizm.mos.ru/inform/detail/3329282.html (дата обращения: 19.03.2023).

11. *Голубкова М.* В Петербурге в общественном транспорте откажутся от кондукторов // RGRU [сайт]. [2021]. URL: https://rg.ru/2021/04/14/reg-szfo/v-peterburge-v-obshchestvennom-transporte-otkazhutsia-ot-konduktorov.html (дата обращения: 19.03.2023).

12. *Зубков И.* Visa и MasterCard прекратили обслуживание четырех российских банков // RGRU [сайт]. [2014]. URL: https://rg.ru/2014/03/21/visa-site.html (дата обращения: 19.03.2023).

13. *Podogreykin.* В России появились проблемы с оплатой через Apple Pay и Google Pay // iPhones.ru [сайт]. [2022]. URL: https://www.iphones.ru/iNotes/AP-GP-02-26-2022 (дата обращения: 19.03.2023).

14. *Fountain Jane E.* Building the Virtual State: Information Technology and Institutional Change. Washington, 2001 [Электронный ресурс] // Google книги [сайт]. [2005]. URL: https://books.google.ru/books?hl=ru&lr=&id=geX4xHFmNMIC&oi=fnd&pg=PR9&dq=digital+state&ots=e44kI8XFwY&sig=83VYsh90KOtxaab554-rmoN7El0&redir_esc=y#v=onepage&q=digital%20state&f=false (дата обращения: 19.03.2023).

15. *Osipov, V.S.* Yellow brick road to digital state // Digital law journal. 2020. Vol. 1. #2. P. 28–40.

16. *Ганиев Р.* Что такое виртуальные государства и почему их нет на карте мира? // Hi-news.ru [сайт]. [2022]. URL: https://hi-news.ru/eto-interesno/chto-takoe-virtualnye-gosudarstva-i-pochemu-ix-net-na-karte-mira.html (дата обращения: 19.03.2023).

17. *Астапенко П.Н.* Демократическое государство и квазигосударственность: институциональные риски в интернет-эпоху // Закон и право. 2018. № 10. С. 15–22.

18. Decenturion.su // Decenturion.su [сайт]. [2019]. URL: https://decenturion.su/ (дата обращения: 19.03.2023).

19. *Баньковский А.Л., Савков П.И.* Концептуальные взгляды стран Запада на кибервойны // Современный мир и национальные интересы Республики Беларусь: матер. Междунар. науч. конф. Минск, 2021. С. 40–45.

20. *Напеева Д.* Аналитики назвали Россию в числе пяти стран с лучшими кибервойсками // РБК [сайт]. [2017]. URL: https://www.rbc.ru/politics/10/01/2017/58747b439a7947526d203417#:~:text=Тройку%20стран%2C%20где%20наиболее%20развиты,настроение%20и%20поведение%20население%20стран» (дата обращения: 19.03.2023).

21. A Q&A with MafiaBoy // InfoSequrity [сайт]. [2013]. URL: https://www.infosecurity-magazine.com/news/a-qa-with-mafiaboy/ (дата обращения: 19.03.2023).

22. Школьник-хакер и DDoS на 2,3 Тбит/с. Топ мощнейших DDoS-атак в мире // Onliner [сайт]. [2020]. URL: https://tech.onliner.by/2020/08/14/top-moshhnejshix-ddos-atak (дата обращения: 19.03.2023).

23. *Царик В.С.* Западная интерпретация информационных конфликтов вокруг Эстонии и Грузии в 2007–2008 гг. в русле концепции «гибридной войны» // Актуальные вопросы современной науки: сборник статей по материалам XVII Международной научно-практической конференции. Уфа, 2018. С. 173–182.

24. *Сарна А.Я.* Взлом матрицы: киберреволюция в Беларуси 2020–2021 гг. // Медиасреда. 2021. № 2. С. 12–18.

6. *Shevchenko, M.* Amazon creates a smart fridge that will keep track of its contents and order its own food [Electronic resource]. *3DNews:* [website]. [2021]. URL: https://3dnews.ru/1050640/amazon-sozdayot-umniy-holodilnik-kotoriy-budet-sledit-za-svoim-sodergimim-i-samostoyatelno-zakazivat-produkti (accessed on: 19.03.2023). (In Rus.).

7. *Zainal, Al N.* The architecture of smart internet of things. T-COM. 2021, 8: 58–61.

8. *Romashkina, N.P., Makhukova, A.V.* Computer virus attack on Iran's nuclear programme. *Informacionnye vojny.* 2013. 4 (28): 88–98. (In Rus.)

9. The most high-profile cyber attacks on critical infrastructure [Electronic resource]. *Habr*: [website]. [2016]. URL: https://habr.com/ru/company/panda/blog/316500/ (accessed on: 19.03.2023). (In Rus.)

10. Property ownership certificate abolished from 15 July. *North Izmaylovo District Administration of Moscow* [website]. [2016]. URL: https://sevizm.mos.ru/inform/detail/3329282.html (accessed on: 19.03.2023). (In Rus.)

11. G*olubkova, M.* St Petersburg will do away with conductors on public transport. *RGRU* [website]. [2021]. URL: https://rg.ru/2021/04/14/reg-szfo/v-peterburge-v-obshchestvennom-transporte-otkazhutsia-ot-konduktorov.html (accessed on: 19.03.2023).

12. *Zubkov, I.* Visa and MasterCard cut service to four Russian banks. *RGRU* [web-site]. [2014]. URL: https://rg.ru/2014/03/21/visa-site.html (accessed on: 19.03.2023).

13. *Podogreykin.* Problems with payment via Apple Pay and Google Pay appeared in Russia. *iPhones.ru* [website]. [2022]. URL: https://www.iphones.ru/iNotes/AP-GP-02-26-2022 (accessed on: 19.03.2023). (In Rus.)

14. *Fountain, Jane E.* Building the Virtual State: Information Technology and Institutional Change. Washington, 2001. *Google knigi* [website]. [2005]. URL: https://books.google.ru/books?hl=ru&lr=&id=geX4xHFmNMIC&oi=fnd&pg=PR9&dq=digital+state&ots=e44kI8XFwY&sig=83VYsh90KOtxaab554-rmoN7El0&redir_esc=y#v=onepage&q=digital%20state&f=false (accessed on: 19.03.2023).

15. *Osipov, V.S.* Yellow brick road to digital state. *Digital law.* 2020. 2: 28–40.

16. *Ganiev, R.* What are virtual states and why aren't they on the world map? *Hi-news.ru* [website]. [2022]. URL: https://hi-news.ru/eto-interesno/chto-takoe-virtualnye-gosudarstva-i-pochemu-ix-net-na-karte-mira.html (accessed on: 19.03.2023). (In Rus.)

17. *Astapenko, P.N.* The Democratic State and Quasi-State: Institutional Risks in the Internet Age. *Zakon i pravo.* 2018. 10: 15–22. (In Rus.)

18. Decenturion.su. *Decenturion.su* [website]. [2019]. URL: https://decenturion.su/ (accessed on: 19.03.2023).

19. *Bankovsky, A.L., Savkov, P.I.* Concluding Views of Western Countries on Cyber Warfare. In: The Modern World and National Interests of the Republic of Belarus: Proceedings of International Scientific Conf. Minsk, 2021: 40-45. (In Rus.)

20. *Napeeva, D.* Analysts named Russia among the five countries with the best cyber forces. RBC [website]. [2017]. *RBC* [website]. [2017]. URL: https://www.rbc.ru/politics/10/01/2017/58747b439a7947526d203417#:~:text=Тройку%20стран%2C%20где%20наиболее%20развиты,настроение%20и%20поведение%20население%20стран» (accessed on: 19.03.2023).

21. A Q&A with MafiaBoy. *InfoSequrity* [website]. [2013]. URL: https://www.infosecurity-magazine.com/news/a-qa-with-mafiaboy/ (accessed on: 19.03.2023).

22. A schoolboy hacker and a 2.3Tbps DDoS. Top of the most powerful DDoS attacks in the world. *Onliner* [website]. [2020]. URL: https://tech.onliner.by/2020/08/14/top-moshhnejshix-ddos-atak (accessed on: 19.03.2023). (In Rus.)

23. *Tsarik, V.S.* Western interpretation of information conflicts around Estonia and Georgia in 2007–2008 in line with the concept of "hybrid warfare". In: *Topical issues of modern science*. Collection of articles on materials of XVII Intern. Sci.-Pract. Conf. Ufa, 2018. P. 173–182.

24. *Sarna, A.Ya.* Hacking the Matrix: Cyber Revolution in Belarus 2020–2021. *Mediasreda*. 2021. No. 2. P. 12–18. (In Rus.)