ОСНОВЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

УДК 338.2 ***EDN WRPWHU***

В.И. Авдийский, А.В. Иванов

ОСОБЕННОСТИ ВЛИЯНИЯ ДЕСТРУКТИВНЫХ СОБЫТИЙ ЦИФРОВОГО ПРОСТРАНСТВА НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ЦИФРОВОГО СУВЕРЕНИТЕТА ГОСУДАРСТВА

Финансовый университет при Правительстве РФ
Москва, Россия

Актуальность исследуемой проблемы обусловлена сложившимся противоречием, заключающееся в том, что с одной стороны цифровизация способствует оптимизации процессов обработки данных, с другой стороны наблюдается рост в цифровом пространстве разрушающих деструктивных событий, влияющих на экономическую безопасность в условиях цифрового суверенитета государства. Представлены инструменты влияния деструктивных событий цифрового пространства на экономическую безопасность, среди которых кибератаки и киберпреступность, кибершпионаж, распространённые вредоносных программ, организация массовых DDoS атак, фейковые новости и дезинформация, нарушение законов о защите персональных данных. Разработаны классификаторы деструктивных моделей цифрового пространства. Предложена модель разрушений интеллектуального агента безопасности автономии, элементами которой являются объекты разрушения, физические и кибератаки на агента, атаки на входные и выходные данные, атаки на систему обучения, каналы и передачи данных агента, средства автоматизации и архитектура системы агента автономии, меры защиты агента. По результатам исследования сформулированы рекомендации органам государственной власти по внедрению модели разрушений интеллектуального агента безопасности автономии деструктивных событий на экономическую безопасность с применением инструментов искусственного интеллекта для защиты экономической безопасности от киберугроз.

Ключевые слова: экономическая безопасность, цифровой суверенитет государства, цифровое пространство, деструктивные события, специальные классификаторы деструктивных событий в области киберугроз, модель разрушений интеллектуального агента безопасности автономии.

Цифровизация экономики. Современный этап развития России характеризуется дальнейшим совершенствованием мероприятий, направленных на институционализацию цифрового суверенитета государства. К их числу следует отнести Указы Президента Российской Федерации, направленные на обеспечение технологической независимости и безопасности критической информационной инфраструктуры [1], а также на реализацию дополнительных мер по обеспечению информационной безопасности Российской Федерации [2]. Кроме того, в Послании Президента Российской Федерации Федеральному Собранию от 29 февраля 2024 года[1] определены стратегические задачи страны до 2030 г. Президент Российской Федерации поручил подготовить национальный проект по формированию экономики данных, а также внедрению управления на основе больших данных. Основа для подобной работы уже заложена: создана инфраструктура цифровой экономики; развиваются электронные экосистемы и онлайн-платформы (например, цифровые платформы «ГосТех» и «Госмаркет») [3]; идет процесс институционализации государственных информационных систем [4]. До 2030 г. будет поддержано не менее 1 тыс. ИТ-стартапов, создано примерно 2 тыс. решений и продуктов, а также подготовлено более 850 тыс. специалистов.[2] Стратегические цели в области цифровой трансформации всех направлений деятельности органов государственной власти востребовали необходимость определения ключевых позиций разрабатываемых классификаторов деструктивных событий цифрового пространства в части обеспечения информационной (в том числе экономической) безопасности. В связи с этим, по поручению Председателя Правительства РФ М. Мишустина были сформированы индустриальные центры компетенций в ключевых отраслях экономики (ИЦК) и центры компетенций по развитию российского общесистемного и прикладного программного обеспечения.[3] Кроме того, осуществляется разработка российских программных решений в экономической сфере по следующим направлениям.

Системы планирования ресурсов предприятия (*ERP*) предназначены для автоматизации и интеграции бизнес-процессов предприятия, управления ресурсами (финансовыми, материальными, человеческими и т.д.), сокращения времени и затрат на выполнение задач, повышения эффективности и прозрачности работы организации. Система *ERP* обеспечивает централизованный доступ к данным и позволяет управлять всеми аспектами деятельности предприятия.

Жизненный цикл изделия (*PLM*) состоит в управлении всеми аспектами жизненного цикла продукта, начиная от его создания и разработки, производства, внедрения на рынок, эксплуатации, обслуживания и до ути-

[1] http://www.kremlin.ru/events/president/transcripts/73585
[2] https://объясняем.рф/articles/news/pasport-natsproekta-ekonomika-dannykh-s-konkretnymi-pokazatelyami-i-rezultatami-budet-podgotovlen-k-/.
[3] https://www.garant.ru/article/1605871/?ysclid=lu04w26l1t428235287

лизации. *PLM* помогает организациям улучшить процессы разработки продукции, сократить время выхода на рынок, повысить качество продукта и управлять всеми изменениями в его жизненном цикле.

Системы управления производственными процессами (*MES*) предназначены для оптимизации и управления производственными операциями в реальном времени. Они помогают повысить производительность, качество продукции, снизить издержки и сократить время производства.

Программно-аппаратные комплексы сбора данных и диспетчерского контроля (*SCADA*) предназначены для мониторинга и управления различными технологическими процессами в реальном времени. Они используются для контроля и управления промышленными объектами, энергетическими системами, системами водоснабжения, транспортом и другими объектами, где важно иметь возможность удаленного мониторинга и управления (рис. 1).

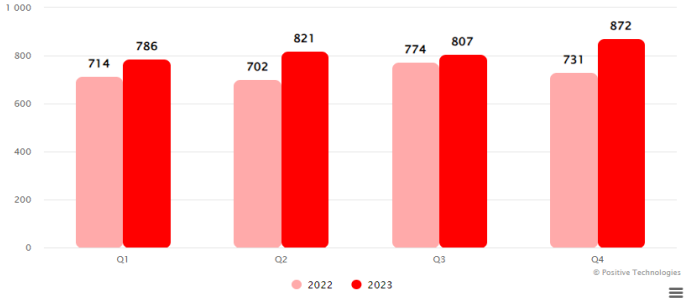
Рис. 1. Направления программных решений в экономической сфере
Источник: составлено авторами

В условиях становления цифрового суверенитета государства важно исследовать процессы, связанные с особенностями влияния деструктивных событий цифрового пространства на общество в целом и на экономическую безопасность, в частности. Например, работа О.В. Карапаева посвящена изучению влияние цифровизации на процесс общественного воспроизводства [5]. В.И. Авдийский, А.В. Иванов и А.В. Царегородцев исследовали синтез классификаторов деструктивных и конструктивных событий цифрового пространства интеллектуального агента безопасности автономии в форме бикубического фасета данных [6]. М.В. Кузнецова изучила механизмы повышения экономической безопасности на основе инновационных и цифровых преобразований в экономике [7]. В работе В.В. Тельбух, А.В. Десятых, С.С. Андрушкевича и Л.В. Пилипенко анализируются методы выявления деструктивного контента в информационных интернет-ресурсах [8]. Однако в вышеперечисленных работах не в полной мере исследуются особенности влияния деструктивных событий цифрового пространства на экономическую безопасность. По нашему мнению, деструктивные события цифрового пространства – это события, которые наносят ущерб информационным системам, данным или ресурсам в сети. Они могут включать в себя кибератаки, хакерские атаки, вирусы, вредоносное программного обеспечения (ПО), фишинг, DDoS-атаки и другие виды киберугроз (рис. 2).

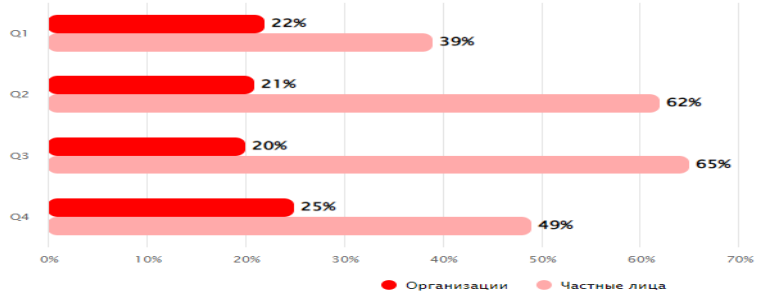
Рис. 2. Структурные элементы цифрового пространства
Источник: составлено авторами

Двойственность цифровизации. В настоящее время в цифровом пространстве обозначилось следующее противоречие. С одной стороны, цифровизация способствует интенсификации процессов сбора, обработки, передачи информации и принятия по ней соответствующих управленческих

решений; с другой стороны, наблюдается рост разрушающих деструктивных событий в цифровом пространстве [8]. Например, по результатам исследования отечественной компании *Positive Technologies* только лишь за 2022-2023 гг. существенно увеличилось количество кибератак в отношении частных лиц и организаций (рис. 3).



а) количество атак в 2022-2023 гг. (по кварталам)



б) доля успешных атак с использованием шпионского ПО

в) методы атак

Рис. 3. Статистика кибератак за период 2022-2023 гг.

Источник: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q4/

Если в 1-м квартале таких атак было 714 (786), то в 4-м – 731 (872) соответственно (рис. 3а). Увеличились атаки с использованием шпионского ПО (рис. 3б). Наконец, возросло количество применяемых методов атаки на организации и частные лица на 10 процентных пунктов (рис. 3в).

Особенности влияния деструктивных событий цифрового пространства на экономическую безопасность. *Экономическая безопасность* включает защиту экономических интересов и обеспечение стабильности экономических процессов от экономических угроз (экономический шпионаж, коррупция, мошенничество и другие формы экономических преступлений). Значительное место в ее обеспечении принадлежит *информационной безопасности*, направленной на защиту конфиденциальности, целостности и доступности информации, а также угроз и атак со стороны злоумышленников.

Базисные классификаторы деструктивных событий цифрового пространства представлены на рис. 4.

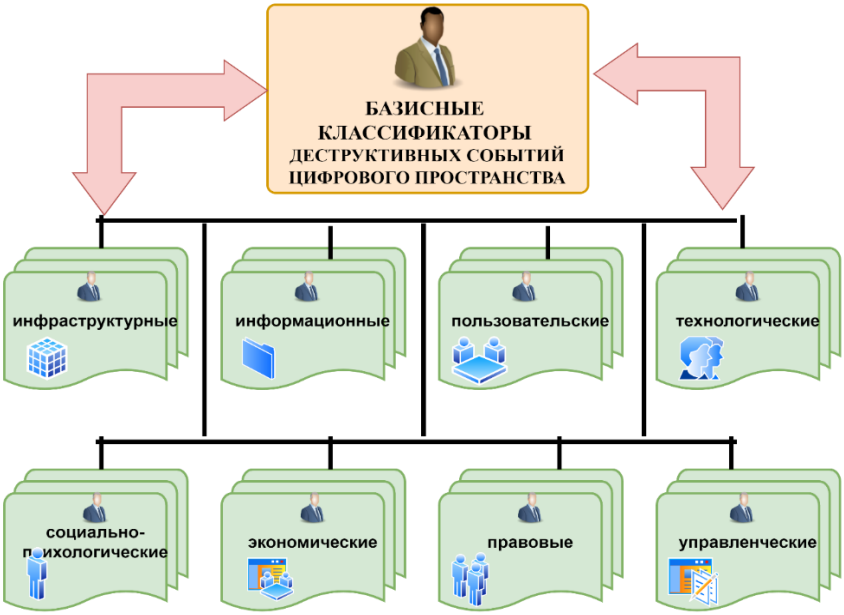


Рис. 4. Базисные классификаторы деструктивных событий цифрового пространства

Источник: составлено авторами

Базисными являются экономические классификаторы, опосредованные влиянием цифровой экономики [9] и такими ее особенностями, как инновационная и цифровая зрелость, цифровая культура и компетенции, циф-

ровая трансформация и цифровое пространство [10]. Структурные элементы *экономических классификаторов* цифрового пространства могут быть организованы следующим образом:

– веб-сайт, мобильное приложение, электронный магазин или платежная система;
– базы данных и хранилища информации для хранения и обработки данных о клиентах, заказах, товарах и услугах;
– интеграция с другими сервисами и платформами для обеспечения полной функциональности и взаимодействия с другими участниками цифрового пространства;
– отчетность и аналитические данные для оценки эффективности и планирования развития бизнеса;
– системы безопасности и защиты данных для обеспечения конфиденциальности и целостности информации в экономической сфере;
– автоматизированные процессы и роботизированные системы для оптимизации работы компании и повышения производительности;
– управление ресурсами и планирование для оптимизации использования ресурсов и улучшения операционной эффективности.

Инструменты влияния деструктивных событий цифрового пространства на экономическую безопасность представлены на рис. 5.

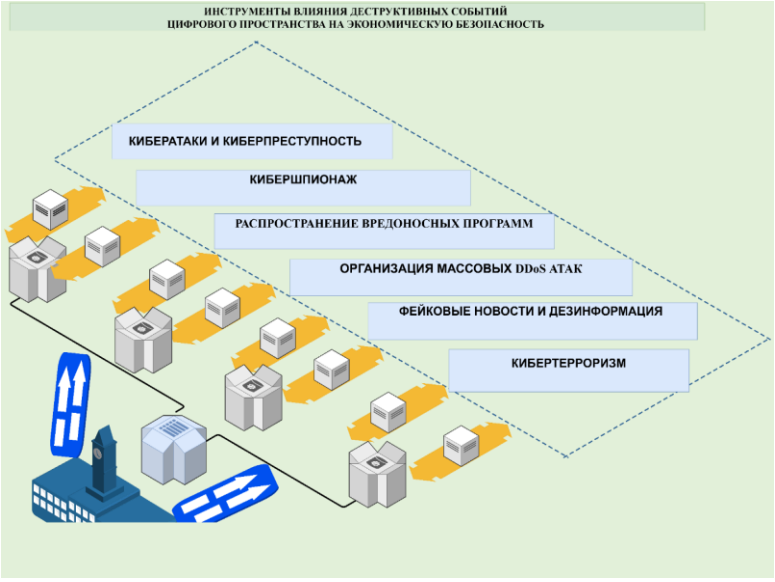


Рис. 5. Инструменты влияния деструктивных событий цифрового пространства на экономическую безопасность

Источник: составлено авторами

***1. Кибератаки и киберпреступность*:** *вредоносное программное обеспечение* – программы, разработанные для внедрения в компьютерные системы с целью нанесения вреда, воровства данных или управления системой без согласия владельца; *фишинг* – метод мошенничества, при котором злоумышленники используют ложные электронные письма или веб-сайты для обмана пользователей и получения конфиденциальной информации; *ДДоС-атаки* – атаки, направленные на перегрузку серверов или сетей, что приводит к отказу в доступе к ресурсам и сервисам; *социальная инженерия* – метод манипуляции людьми с целью получения конфиденциальной информации или доступа к системам; *вредоносные рекламные программы* – программы, которые незаметно устанавливаются на компьютер пользователя и могут использоваться для кражи данных или отслеживания действий пользователя; *уязвимости программного обеспечения* – неисправности в программном обеспечении, которые могут быть использованы злоумышленниками для внедрения в систему и проведения кибератак.

2. Кибершпионаж: *взлом компьютерных систем и сетей предприятий* для получения конфиденциальной информации о финансах, технологиях и бизнес-планах; *кража интеллектуальной собственности* через вирусы, трояны и другие вредоносные программы; *отслеживание и мониторинг деятельности конкурентов*, включая их стратегии, клиентов и партнеров; *распространение дезинформации и фейковых новостей* для дестабилизации рынка и обесценивания активов; *подделка документов и электронных сообщений* с целью проведения мошеннических операций; *вымогательство и шантаж* с использованием угроз разглашения конфиденциальной информации; *создание ботнетов для массовых атак на финансовые учреждения* и корпорации; *уязвимости в критической инфраструктуре*, такие как энергетика, транспорт и связь, которые могут быть использованы для проведения кибератак.

3. Распространение вредоносных программ: *вредоносные программы* могут шифровать данные на компьютере или в сети предприятия и требовать выкуп за их расшифровку; использоваться для кражи конфиденциальных данных, таких как финансовые отчеты, планы развития, интеллектуальная собственность и другая чувствительная информация; модифицировать данные в банковских системах или электронных платежных системах, совершать незаконные транзакции и мошеннические операции; использованы для саботажа работы компьютеров, сетей и систем предприятия, что приведет к простоям в работе и потере доходов; направлены на вывод клиентов на мошеннические сайты или заражение компьютеров рекламными вредоносными программами. Это может привести к утечкам финансовых данных, к установке дополнительных вредоносных программ и другим проблемам, которые негативно отразятся на экономической безопасности предприятия.

4. Организация массовых DDoS атак: *злоумышленники могут использовать ботнеты*, состоящие из компьютеров и устройств, зараженных вредоносными программами, для организации массовых *DDoS* атак. Это может привести к перебоям в работе онлайн-сервисов и веб-сайтов компаний, что может негативно отразиться на их бизнесе; *DDoS атаки могут быть направлены на ключевые сетевые узлы и сервисы компании,* что может привести к сбоям в работе сети и сервисов, а также к потере клиентов и доходов, а также нанести серьезный ущерб репутации компании; *простои в работе и потеря клиентов из-за DDoS атак* могут привести к значительным *финансовым потерям для компании*, особенно если атака продолжается длительное время и не удается своевременно восстановить работоспособность сервисов; для защиты от *DDoS* атак компании могут вынуждены *тратить дополнительные средства на приобретение и поддержание специализированных систем защиты*, что также может сказаться на экономической безопасности.

5. Фейковые новости и дезинформация: создание ложной информации и вымышленных событий, которые могут повлиять на решения бизнесменов и инвесторов; распространение дезинформации о финансовых рынках, компаниях и отраслях, что может привести к панике среди инвесторов и снижению цен на акции; использование фейковых новостей для манипуляции курсами валют и товаров на рынке; провокация конфликтов и нестабильности в экономике через распространение ложной информации о политических и экономических событиях; создание искусственных кризисов в экономике с помощью дезинформации о финансовых институтах или компаниях; взаимодействие с компрометированными журналистами и блогерами для распространения ложной информации; создание ложных рекламных кампаний и пропаганды, которые могут ввести потребителей в заблуждение относительно продуктов и услуг, что может привести к убыткам для компаний.

6. Нарушение законов о защите экономических (персональных) данных: незаконный сбор и использование персональных данных без согласия субъектов данных, что может привести к нарушению конфиденциальности и приватности, а также к утечкам информации о клиентах и партнерах; утечка и недостаточная защита персональных данных, что может привести к утечкам конфиденциальной информации о клиентах, партнерах и сотрудниках, а также к нарушению законодательства о защите данных; нарушения в области кибербезопасности, такие как хакерские атаки, вирусы и вредоносное ПО, которые могут привести к утечкам конфиденциальной информации, краже данных и финансовым потерям; нарушения в области безопасности информационных систем, такие как недостаточная защита от внешних угроз и несанкционированный доступ к данным, что может привести к

утечкам и краже конфиденциальной информации; использование недостоверных данных и информации в бизнес-процессах, что может привести к ошибкам в принятии решений, потере клиентов и ущербу для компании.

7. Кибертерроризм: кибератаки на финансовые институты, такие как банки и платежные системы, с целью вымогательства, кражи денег или нарушения работы системы платежей, что может привести к финансовым потерям и потере доверия со стороны клиентов; кибератаки на крупные корпорации и компании для кражи конфиденциальной информации, интеллектуальной собственности и коммерческих секретов, что может привести к утечкам данных, финансовым убыткам и потере конкурентного преимущества; кибертерроризм на системы критической инфраструктуры, такие как энергетические объекты, транспортные системы и коммуникационные сети, с целью нарушения их работы или даже причинения физических ущербов, что может привести к экономическим потерям и угрозе безопасности страны; кибертерроризм на онлайн-торговые платформы и интернет-магазины с целью блокировки работы сайта, кражи финансовых данных клиентов или искажения информации о продуктах и услугах, что может привести к убыткам для бизнеса и потере доверия со стороны клиентов; организация киберпропаганды и дезинформации с использованием социальных сетей и интернет-ресурсов для манипуляции общественным мнением и создания хаоса в экономике, что может привести к панике среди населения и инвесторов, а также к убыткам для бизнеса и финансовым потерям.

Классификаторы деструктивных событий. По результатам анализа классификаторов деструктивных событий выявлены следующие типы подобных нарушителей.

1. *Нарушители, обладающие базовыми возможностями,* которые владеют компьютерными знаниями и навыками на уровне пользователя. К числу таких нарушителей относятся: физические лица (хакеры); лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем; авторизованные пользователи систем и сетей, а также бывшие работники (пользователи).

2. *Нарушители, обладающие повышенными возможностями,* которые имеют возможность использовать средства реализации угроз (инструменты), владеют фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей, обладают практическими знаниями о операционных систем. К таким нарушителям относятся: преступные группы; конкурирующие организации и др.

3. *Нарушители, обладающие высокими возможностями,* которые имеют возможность получения доступа к исходному коду встраиваемого программного обеспечения аппаратных платформ, системного и прикладного программного обеспечения для получения сведений об уязвимостях, имеют возможность внедрения программных (программно-аппаратных) за-

кладок или уязвимостей на различных этапах поставки программного обеспечения или программно-аппаратных средств. К таким нарушителям относятся: террористические, экстремистские группировки, а также разработчики программных, программно-аппаратных средств.

Сводная таблица классификаторов деструктивных событий цифрового пространства представлена на рис. 6.

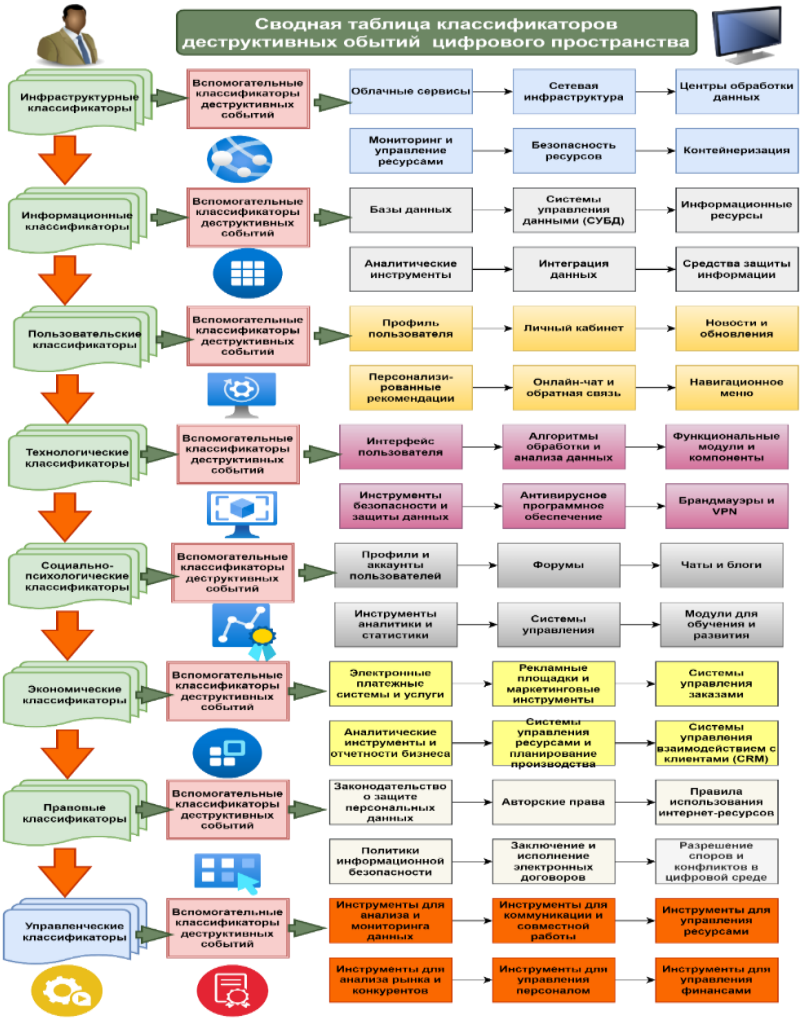


Рис. 6. Сводная таблица классификаторов деструктивных событий цифрового пространства

Источник: составлено авторами

В России существуют следующие классификаторы деструктивных событий в цифровом пространстве. *Классификатор угроз информационной безопасности,* который разработан Федеральной службой безопасности (ФСБ) России и определяет различные типы информационных угроз, такие как хакерские атаки, распространение вредоносного программного обеспечения, кибершпионаж и др. *Классификатор атак и инцидентов информационной безопасности,* разработанный Центром информационной безопасности (ЦИБ) ФСБ России, который описывает различные виды атак и инцидентов в цифровом пространстве. *Классификатор информационных технологий*, применяемых при организации работ по обеспечению информационной безопасности, разработанный Федеральной службой по техническому и экспортному контролю (ФСТЭК) России, который определяет информационные технологии, используемые при обеспечении информационной безопасности. *Национальный классификатор угроз информационной безопасности,* разработанный ФСБ России и определяющий различные типы угроз информационной безопасности, включая информацию о методах атак, уязвимостях систем, инцидентах и технических мерах обеспечения безопасности информации. *Специальные классификаторы деструктивных событий в области киберугроз.* В общем виде специальные классификаторы деструктивных событий в области киберугроз представлены на рис. 7.

Рис. 7. Специальные классификаторы деструктивных событий в области киберугроз

Источник: составлено авторами

Модель разрушений интеллектуального агента безопасности автономии. Предложенные выше классификаторы деструктивных событий цифрового пространства способствовали разработке *модели разрушений интеллектуального агента безопасности автономии (ИАБА).* Целью подобной модели являются выявление и анализ потенциальных слабых мест и уязвимостей автономных агентов, а также разработка мер безопасности и защиты для предотвращения подобных угроз. Ключевым понятием подобной модели является *интеллектуальный агент безопасности автономии (агент автономии)*, который должен: обнаруживать потенциальные угрозы и атаки на систему автономии; реагировать на обнаруженные угрозы и атаки; обучаться на основе новой информации и адаптироваться к изменяющемуся цифровому пространству; непрерывно мониторить состояние безопасности и предоставлять отчеты о результатах своей работы; осуществлять взаимодействие между различными интеллектуальными агентами безопасности.

Структурные элементы модели разрушений интеллектуального агента безопасности автономии представлены на рис. 8.

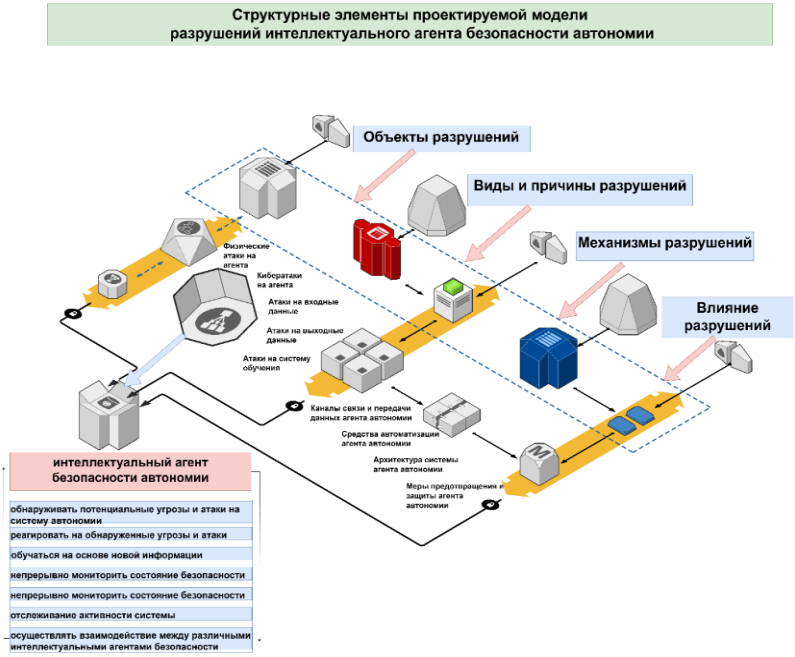


Рис. 8. Структурные элементы модели разрушений интеллектуального агента безопасности автономии

Источник: составлено авторами

Рассмотрим структурные элементы проектируемой модели разрушений интеллектуального агента безопасности автономии.

1. *Объекты разрушения* – часть интеллектуального агента, которая может быть подвержена разрушению. Таковыми могут быть: *модуль сбора, обработки и интерпретации данных,* получаемых от датчиков или других источников информации; *модуль принятия решений,* в котором агент анализирует собранные данные и решает, какие действия следует предпринять; *модуль связи со внешними системами*, отвечающий за обмен данными и коммуникацию с другими системами или агентами; *физические компоненты*, такие как процессоры, память, датчики и пр.

Виды разрушений модели интеллектуального агента безопасности автономии могут включать следующие характеристики:

- *физические атаки*, приводящие к физическому повреждению агента;
- *электронные атаки* – атаки на электронные системы агента, такие как взлом или перехват сигналов;
- *алгоритмические атаки* – изменение или нарушение работы алгоритмов, используемых агентом для принятия решений;
- *социальные атаки* – манипуляция другими агентами или людьми для введения агента в заблуждение или изменения его поведения;
- *внутренние атаки* – изменение программного обеспечения или аппаратных компонентов агента с целью нарушения его надежности или безопасности.

Причины разрушений модели интеллектуального агента безопасности автономии могут быть следующими:

- *ошибки в проектировании*, по причине которых агент может быть уязвим для различных видов атак или разрушений;
- *нехватка ресурсов,* таких как энергия, вычислительная мощность или связь;
- *недостаток информации или обучения,* приводящий к тому, что в случае недостаточной информации агент может не иметь полного представления о своей роли и обязанностях в обеспечении безопасности.

Механизмы разрушений проектируемой модели могут включать следующие характеристики: вирусы и вредоносные программы, взломанные устройства, фальшивые данные, физические атаки, социальная инженерия, с применением которой злоумышленники могут попытаться манипулировать агентом или его акторами, чтобы изменить его поведение.

Влияние разрушений имеет следующие характеристики: перебор возможных атак, повреждение функциональности, утечка конфиденциальных данных, нарушение целостности в результате чего агент может быть перепрограммирован.

2. *Физические атаки на агента*, включающие физическое его повреждение, блокировку работы или физическое вмешательство по функционированию агента, например, переключение переключателей, размещение препятствий или манипулирование его датчиками.

3. ***Кибератаки на агента,*** методами которых являются: внедрение вирусов и вредоносного ПО для отключения или взлома системы безопасности; отказ в обслуживании (*DDoS*) для перегрузки и блокировки системы.

4. ***Атаки на входные данные,*** которые описывают манипулирование входными данными для принятия решений. К числу таких атак можно отнести: внедрение некорректных или искаженных данных для искажения результатов анализа безопасности и принятия решений агентом; манипуляция данными для обмана и обхода системы безопасности; внедрение сбоев или ошибок во входные данные для вызова нежелательного поведения агента или создания путаницы в системе безопасности.

5. ***Атаки на выходные данные,*** предусматривающие искажение выходных данных автономного агента, что может привести к неправильным действиям или решениям. Признаками подобной атаки являются: манипуляция или изменение результатов анализа и принятия решений безопасности агентом; вывод ложной или искаженной информации для создания ложного впечатления о состоянии безопасности; внедрение аномальных или вредоносных действий в реакции на полученные выходные данные.

6. ***Атаки на систему обучения и принятия решений автономного агента,*** основанных на подборе вредоносных обучающих данных или атакой на алгоритмы принятия решений. Методами такой атаки являются: внедрение ошибочных или ложных данных для искажения процесса обучения и вывода недостоверных результатов; отказ в обучении путем блокировки доступа к обучающим данным или изменения параметров обучения; манипуляция функциями потерь или критериями оценки качества обучения для изменения поведения и решений агента безопасности.

7. ***Каналы связи и передачи данных агента*** *автономии* обеспечивают передачу информации между различными его компонентами агента, а также между агентом и операторами системы безопасности. Такими каналами являются: беспроводные каналы связи, такие как *Wi-Fi*, *Bluetooth*, NFC и др.; проводные каналы связи, например, *Ethernet*, *USB*, *HDMI* и т.д.; облачные сервисы и хранилища данных для обмена информацией и обновлений; локальные сети и интранет для обмена данных внутри автономной системы.

8. ***Средства автоматизации агента автономии*** включают в себя программное и аппаратное обеспечение для автоматизации процессов мониторинга, анализа и принятия решений, что повышает эффективность деятельности агента безопасности.

9. ***Архитектура системы агента автономии,*** включающая:

- сенсоры и датчики, необходимые для принятия решений агентом;
- процессор и вычислительные ресурсы, обрабатывающие собранные данные, а также запускающие алгоритмы и модели машинного обучения для принятия решений;
- модуль обучения и адаптации, отвечающий за обучение агента, анализ данных, выявление паттернов и улучшение его способностей через обратную связь;

- модуль принятия решений, который на основе полученных данных и обучения принимает автономные решения в реальном времени;
- модуль управления и выполнения задач – координирует действия агента, взаимодействует с другими системами, управляет процессами выполнения задач;
- база знаний и хранилище данных – содержит информацию, модели, алгоритмы, историю действий и обучения, необходимые для работы агента;
- модуль безопасности – обеспечивает защиту агента от внешних угроз, обработку уязвимостей, контроль доступа и управление данными агента.

10. ***Меры предотвращения и защиты агента автономии*** могут включать кодирование и шифрование данных, которые помогают предотвратить несанкционированный доступ. Для этого применяются следующие программно-аппаратные средства защиты информации:

- криптографические алгоритмы, криптографические ключи, шифровальные устройства, смарт-карты – пластиковые карты с встроенными микроконтроллерами и криптографическими функциями;
- токены безопасности – флэш-накопители, которые хранят и генерируют криптографические ключи и предоставляют доступ к защищенным системам;
- системы аутентификации, используемые для проверки подлинности пользователей перед предоставлением доступа к защищенным данным.

Для установления строгих правил доступа к информации применяются следующие программно-аппаратные средства защиты:

- *системы управления доступом* (СУД) – программные и аппаратные компоненты, которые управляют доступом пользователей к информационным ресурсам;
- *брендмауэры* – аппаратные и программные устройства, которые контролируют и регулируют трафик между сетями;
- *прокси-серверы* – серверы, которые принимают запросы от клиентов и перенаправляют их к запрашиваемым ресурсам;
- *системы идентификации и аутентификации* – программные и аппаратные средства, которые проверяют личность и подлинность пользователей перед предоставлением им доступа к информационным ресурсам;
- *системы контроля целостности* – программные и аппаратные компоненты, которые проверяют целостность файлов и информационных ресурсов;
- *цифровые подписи* – технологии, которые позволяют проверить подлинность и целостность сообщений и данных.

Для *аудита безопасности информации* применяются следующие программно-аппаратные средства защиты:

- *системы журналирования* – программные и аппаратные системы записывают события и активности системы;

- *мониторинг систем,* который основан на применении средств для наблюдения за активностью системы или сети, а также для обнаружения аномального поведения или вторжений;
- *системы обнаружения вторжений* (СОВ) – программно-аппаратные средства, которые мониторят сетевой трафик и системные журналы для обнаружения атак, эксплойтов и других форм вторжений в компьютерные системы;
- *системы анализа безопасности* – программные и аппаратные средства проводят комплексный анализ безопасности компьютерных систем и сетей;
- *протоколирование и мониторинг целостности данных* – средства позволяют обеспечить непрерывное протоколирование и мониторинг целостности данных и обнаруживать любые попытки изменить или повредить данные.

Для мониторинга и реагирования на информационные инциденты используются различные программно-аппаратные средства. Некоторые из них включают в себя:

- *SIEM* (*система управления информационной безопасностью и событиями*) – программно-аппаратную систему, которая собирает, анализирует и реагирует на данные безопасности и событий из различных источников, таких как журналы аудита, системы обнаружения вторжений, межсетевые экраны и другие системы безопасности;
- *IDS* (*системы обнаружения вторжений*) – контролируют сетевой трафик на наличие аномалий или подозрительных активностей, используя сигнатуры или другие методы анализа, могут оповещать о возможных атаках или инцидентах, чтобы операторы безопасности могли принять соответствующие меры;
- *IPS (системы предотвращения вторжений)* – контролируют сетевой трафик, но они также могут автоматически реагировать на обнаруженные угрозы и блокировать соответствующий трафик с помощью маршрутизации или других подобных методов;
- *EDR* (*Endpoint Detection and Response*) – программно-аппаратные системы, которые устанавливаются на конечные устройства, такие как компьютеры или серверы, и непрерывно контролируют их активность с целью обнаружения и предотвращения инцидентов безопасности. Все эти программно-аппаратные средства помогают обнаруживать инциденты безопасности, мониторировать активность, реагировать на угрозы и предотвращать дальнейшие атаки или инциденты.

Модель автономии интеллектуального агента безопасности. На рис. 9 представлены структурные элементы модели автономии интеллектуального агента безопасности автономии в органах государственной власти. Она содержит следующие структурные элементы.

1. *Автономные алгоритмы и программное обеспечение*, используемые для обработки и анализа информации, принятия решений и выполнения задач без прямого вмешательства оператора.

2. *Штатное и аппаратное обеспечение*, включающее компьютеры, серверы, сетевое оборудование, устройства сбора данных, датчики и другие технические средства, необходимые для работы и функционирования агента.

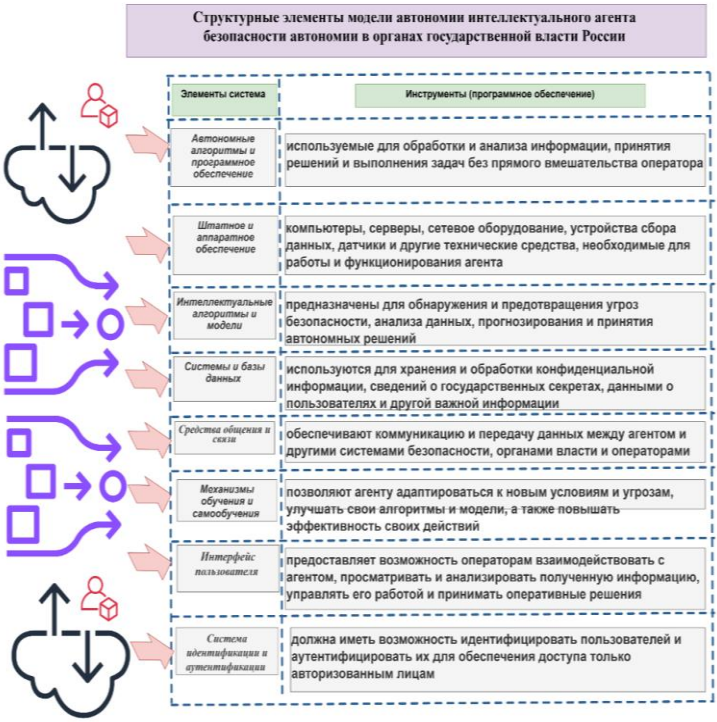


Рис. 9. Структурные элементы модели автономии интеллектуального агента безопасности автономии в органах государственной власти России
Источник: составлено авторами

3. *Интеллектуальные алгоритмы и модели,* которые предназначены для обнаружения и предотвращения угроз безопасности, анализа данных, прогнозирования и принятия автономных решений.

4. *Системы и базы данных* – используются для хранения и обработки конфиденциальной информации, сведений о государственных секретах, данными о пользователях и другой важной информации.

5. *Средства общения и связи* – обеспечивают коммуникацию и передачу данных между агентом и другими системами безопасности, органами власти и операторами.

6. *Механизмы обучения и самообучения* позволяют агенту адаптироваться к новым условиям и угрозам, улучшать свои алгоритмы и модели, а также повышать эффективность своих действий.

7. *Механизмы контроля и самооценки* обеспечивают возможность агенту проверять и оценивать свою работу, выявлять потенциальные ошибки и недостатки, а также корректировать свое поведение.

8. *Интерфейс пользователя* предоставляет возможность операторам взаимодействовать с агентом, просматривать и анализировать полученную информацию, управлять его работой и принимать оперативные решения.

9. Система идентификации и аутентификации должна иметь возможность идентифицировать пользователей и аутентифицировать их для обеспечения доступа только авторизованным лицам.

Рекомендации органам государственной власти по внедрению модели разрушений интеллектуального агента безопасности автономии следующие.

1. Внедрение в модель разрушений интеллектуального агента безопасности автономии инструментов искусственного интеллекта (ИИ) для защиты от *DDoS*-атак по следующим направлениям: использование алгоритмов ИИ, которые могут интерпретировать большие объемы трафика, позволяют блокировать вредоносную деятельность; интеллектуальные алгоритмы на основе множественных показателей, позволяющие проводить самодиагностику и раннее обнаружение неисправностей для обеспечения наибольшей непрерывной работы; поиск причин появления неисправностей на основе обработки больших объемов данных.

2. Внедрение в модель разрушений интеллектуального агента безопасности автономии методологии анализа корреляции данных о деструктивных событиях от приведения собираемых данных к единому формату до вычисления степени важности результатов процесса корреляции.

3. Совершенствование инструментов обнаружения и предотвращения атак в модели разрушений интеллектуального агента безопасности автономии на основе внедрения программно-аппаратных средств защиты для анализа безопасности атак в модели разрушений интеллектуального агента безопасности автономии программного комплекса *SIEM*, предназначенного для сбора и анализа логов, событий и данных безопасности с различных источников, позволяя выявлять и реагировать на атаки в режиме реального времени.

4. В органах государственной власти целесообразно внедрять технологию разработки классификаторов деструктивных событий цифрового пространства и создание на ее основе соответствующих их стандартов. Разработка классификационной системы модели разрабатываемых классификаторов деструктивных событий цифрового пространства в органах государ-

ственной власти, включающая следующую последовательность: определение основных целей и требований классификационной системы, таких как обнаружение различных типов деструктивных событий, точность и эффективность работы системы, интеграция с существующими системами безопасности и т.д.; сбор и подготовка данных из различных источников, таких как журналы событий, доклады о нарушениях безопасности, жалобы пользователей и другие; анализ предварительно подготовленных данных с помощью различных методов и алгоритмов; разработка классификаторов, которые позволяют отличать деструктивные события от нормальной активности; тестирование и оценка классификационной системы; внедрение классификационной системы в органах государственной власти.

Библиографический список

[1] Указ Президента РФ от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. URL: http://publication.pravo.gov.ru /Document/View/0001202203300001?ysclid=lysk37kunp148752373

[2] Указ Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [Электронный ресурс]. URL: http://publication.pravo.gov.ru /Document/View/0001202205010023?ysclid=lysk582cib801123184

[3] Постановление Правительства РФ от 30 ноября 2022 г. № 2194 «Об утверждении Положения о федеральной государственной информационной системе «Управление единой цифровой платформой Российской Федерации «ГосТех» и Положения о федеральной государственной информационной системе «Госмаркет» (с изменениями и дополнениями)» [Электронный ресурс]. URL: https://base.garant.ru/405875901/?ysclid=lyskba5q4w936167619

[4] Иванов А.В. Становление и институционализация государственных информационных систем. Международный научный журнал "Вектор научной мысли" 2023. № 3 (3). [Электронный ресурс]. URL: https://vektornm.ru/files/Ivanov_Anatoliy_Viktorovich.pdf

[5] Карапаев О.В. Влияние цифровизации на процесс общественного воспроизводства. Автореф. дис ... уч. степ. канд. экон. наук. М., 2022. [Электронный ресурс]. URL: https://inecon.org/docs/2022/Karapaev_avtoreferat.pdf?ysclid=lysknstzvl915657182

[6] Коротков А.В. Преодоление цифрового неравенства как информационная стратегия современного общества. Автореф. дис… уч. степ. канд. филол. наук. М., 2023.

[7] Метод выявления деструктивного контента в информационных интернет-ресурсах / В.В. Тельбух, А.В. Десятых, С.С. Андрушкевич, Л.В. Пилипенко // Известия ТулГУ. Технические науки. 2023. Вып. 3. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/metod-vyyavleniya-destruktivnogo-kontenta -v-informatsionnyh-internet-resursah?ysclid=lyslq03egm289005798

[8] Цифровая экономика: 2022: краткий статистический сборник / Г.И. Абдрахманова, С.А. Васильковский, К.О. Вишневский и др.; Нац. исслед. ун-т «Высшая школа экономики». М.: НИУ ВШЭ, 2022. 124 с.

[9] Ячменева В.М., Ячменев Е.Ф. Цифровое пространство как необходимое и достаточное условие цифровизации экономики. Baikal Research Journal электронный научный журнал Байкальского государственного университета. 2020. Т. 11, № 3. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/tsifrovoe-prostranstvo-kak-neobhodimoe-i-dostatochnoe-uslovie-tsifrovizatsii-ekonomiki?ysclid=lysmclrgek683842922

V.I. Avdiysky, A.V. Ivanov

THE FEATURES OF THE INFLUENCE OF DESTRUCTIVE EVENTS IN THE DIGITAL SPACE ON THE ECONOMIC SECURITY IN CONDITIONS OF THE DIGITAL SOVEREIGNTY OF THE STATE

Financial University under the Government of the Russian Federation
Moscow, Russia

Abstract. The relevance of the problem under study is due to the existing contradiction, which consists in the fact that, on the one hand, digitalization contributes to the optimization of data processing processes, on the other hand, there is an increase in the digital space of destructive events that affect economic security in the context of the digital sovereignty of the state. The paper presents tools for the influence of destructive events in the digital space on economic security, including cyber attacks and cybercrime, cyber espionage, widespread malware, organization of mass DDoS attacks, fake news and disinformation, violation of laws on the protection of personal data. Classifiers of destructive models of the digital space have been developed. A model of destruction of an intelligent autonomy security agent is proposed, the elements of which are objects of destruction, physical and cyber attacks on the agent, attacks on input and output data, attacks on the training system, agent channels and data transmission, automation tools and the architecture of the autonomy agent system, agent protection measures. Based on the results of the study, recommendations were formulated for government bodies on the implementation of the model of destruction of the intelligent agent of autonomy security of destructive events on economic security using artificial intelligence tools to protect economic security from cyber threats.

Key words: economic security, digital sovereignty of the state, digital space, destructive events, special classifiers of destructive events in the field of cyber threats, model of destruction of the intelligent agent of autonomy security.

References

[1] Decree of the President of the Russian Federation of March 30, 2022 No. 166 “On measures to ensure technological independence and security of the critical information infrastructure of the Russian Federation” [Electronic resource]. Available at: http:// publication.pravo.gov.ru /Document/View/0001202203300001?ysclid=lysk37kunp148752373

[2] Decree of the President of the Russian Federation of May 1, 2022 No. 250 “On additional measures to ensure information security of the Russian Federation” [Electronic resource]. Available at: http://publication.pravo.gov.ru /Document/View/0001202205010023?ysclid=lysk582cib801123184

[3] Decree of the Government of the Russian Federation of November 30, 2022 No. 2194 "On approval of the Regulations on the federal state information system "Management of the unified digital platform of the Russian Federation "GosTech" and the Regulations on the federal state information system "GosMarket" (with changes and additions)” [Electronic resource]. Available at: https://base.garant.ru/405875901/?ysclid=lyskba5q4w936167619

[4] Ivanov, A.V. (2023). [Formation and institutionalization of state information systems]. *Mezhdunarodnyj nauchnyj zhurnal "Vektor nauchnoj mysli"* [International scientific journal "Vector of Scientific Thought"]. No. 3 (3). [Electronic resource]. Available at: https://vektornm.ru/files/Ivanov_Anatoliy_Viktorovich.pdf

[5] Karapaev, O.V. (2022). [The impact of digitalization on the process of social reproduction]. [Electronic resource]. Available at: https://inecon.org/docs/2022/Karapaev_avtoreferat.pdf?ysclid=lysknstzvl915657182

[6] Korotkov, A.V. (2023). [Overcoming the digital divide as an information strategy of modern society]. *M* [M]. (In Russ).

[7] Telbukh, V.V., Desyatykh, A.V., Andrushkevich, S.S., Pilipenko, L.V. (2023). [The method for identifying destructive content in Internet information resources]. *Izvestija TulGU. Tehnicheskie nauki* [News of Tula State University. Technical science]. [Electronic resource]. Available at: https://cyberleninka.ru/article/n/metod-vyyavleniya-destruktivnogo-kontenta-v-informatsionnyh-internet-resursah?ysclid=lyslq03egm289005798

[8] Abdrakhmanova, G.I. (2022). [Digital economy: 2022: a brief statistical collection]. *M.: NIU VShJe* [M.: National Research University Higher School of Economics]. 124 p. (In Russ).

[9] Yachmeneva, V.M., Yachmenev, E.F. (2020). [Digital space as a necessary and sufficient condition for the digitalization of the economy]. *Jelektronnyj nauchnyj zhurnal Bajkal'skogo gosudarstvennogo universiteta* [Electronic scientific journal of Baikal State University]. [Electronic resource]. Available at: https://cyberleninka.ru/article/n/tsifrovoe-prostranstvo-kak-neobhodimoe-i-dostatochnoe-uslovie-tsifrovizatsii-ekonomiki?ysclid=lysmclrgek683842922