# Стратегическое управление кибербезопасностью

**Буди Гунаван**
Профессор, Программа исследований в области кибербезопасности (Cyber Security Study Program), budigunawan@stin.ac.id

**Барито Мульо Ратмоно**
Заместитель руководителя, Программа исследований в области технологической разведки (Technology of Intelligence Study Program), barito.mr@stin.ac.id

Университет Sekolah Tinggi Intelijen Negara, Индонезия, 9VQQ+6J2, Sumur Batu, Kec. Babakan Madang, Kabupaten Bogor, Jawa Barat 16810, Indonesia

**Аде Гафар Абдулла**
Профессор, Программа исследований в области технологического и профессионального образования (Technological and Vocational Education Study Program), ade_gaffar@upi.edu

Университет Pendidikan (Universitas Pendidikan), Индонезия, Jl. Dr. Setiabudi No. 229, Isola, Kec. Sukasari, Kota Bandung, Jawa Barat 40154, Indonesia

## Аннотация

На фоне динамичного развития технологий и усложнения коммуникационных сетей актуализируется проблема кибербезопасности, становящаяся ключевым аспектом стратегического планирования. Защищенность информационных, финансовых, репутационных и других активов от все более частых и изощренных кибератак зависит от умения разрабатывать и постоянно обновлять комплексный, упреждающий подход с учетом широкого спектра факторов. Состояние национальной кибербезопасности стало одним из ключевых индикаторов уровня развития наряду с «классическими» показателями (ВВП и т. п.). Возникшее недавно исследовательское направление «экономика кибербезопасности» постоянно обогащается новыми знаниями и подходами.

В статье анализируются риски для системы кибербезопасности на разных уровнях и основные меры по ее укреплению, оценивается динамика управленческих тенденций. Обозначены ключевые компетенции, актуальные для профессионалов рассматриваемой сферы.

**Ключевые слова:** кибербезопасность; разведка; стратегическое управление; управление рисками; библиометрический анализ

**Цитирование:** Gunawan B., Ratmono B.M., Abdullah A.G. (2023) Cyber Security and Strategic Management. *Foresight and STI Governance*, 17(3), 88–97. DOI: 10.17323/2500-2597.2023.3.88.97

# Cyber Security and Strategic Management

**Budi Gunawan**
Professor, Cyber Security Study Program, budigunawan@stin.ac.id

**Barito Mulyo Ratmono**
Deputy Governor, Technology of Intelligence Study Program, barito.mr@stin.ac.id

Sekolah Tinggi Intelijen Negara, 9VQQ+6J2, Sumur Batu, Kec. Babakan Madang, Kabupaten Bogor, Jawa Barat 16810, Indonesia

**Ade Gafar Abdullah**
Professor, Technological and Vocational Education Study Program, ade_gaffar@upi.edu

Universitas Pendidikan Indonesia, Jl. Dr. Setiabudi No. 229, Isola, Kec. Sukasari, Kota Bandung, Jawa Barat 40154, Indonesia

## Abstract

Against the backdrop of rapidly evolving technologies and increasingly complex communications networks, cybersecurity is becoming a key aspect of strategic planning. Protecting information, financial, reputational and other assets from increasingly frequent and sophisticated cyberattacks depends on the ability to develop and continually update a comprehensive, proactive approach that takes into account a wide range of factors. The state of national cybersecurity has become one of the key indicators of the level of development along with «classic» indicators (GDP, etc.). The recently emerged research area of «cybersecurity economics» is constantly being enriched with new knowledge and approaches.

The article analyzes the risks to the cybersecurity system at different levels and the main measures to strengthen it, and assesses the dynamics of management trends. Key competencies relevant for professionals in this field are outlined.

**Keywords:** cybersecurity; intelligence; strategic management; risk management; bibliometrics analysis

**Citation:** Gunawan B., Ratmono B.M., Abdullah A.G. (2023) Cyber Security and Strategic Management. *Foresight and STI Governance*, 17(3), 88–97. DOI: 10.17323/2500-2597.2023.3.88.97

По мере того, как предприятия все активнее переводят операции в онлайн, в цифровой сфере активизируется киберпреступность[1]. Для противодействия этому деструктивному тренду развивается и совершенствуется сфера кибербезопасности, предлагающая меры по защите от кибератак и экономического шпионажа. Изначально ее организация воспринималась лишь как «проблема управления ИТ». Однако ввиду расширения масштабов внешних угроз и востребованности защитных мер вопрос кибербезопасности приобрел не только стратегическое, но также технологическое и юридическое значение (Mantha, de Soto, 2021). Несмотря на динамичный технологический прогресс, основную роль в защите от киберугроз по-прежнему играет человек, определяющий стратегию борьбы с ними. Алгоритмы нередко принимают ошибочные решения, их функционированию недостает прозрачности, следовательно, уверенность в эффективности таких механизмов, как правило, необоснована. Стратегия «Общество 5.0», инициированная в Японии, направлена на оптимизацию управления технологиями с учетом человеческого фактора[2]. Согласно лежащей в ее основе концепции «интеллектуального общества», физическое и цифровое пространства тесно переплетены. По сравнению с «Индустрией 4.0», которая, прежде всего, ориентирована на автоматизацию производственных процессов, «Общество 5.0» предполагает более глубокую интеграцию технологий с общественными ценностями в целях создания новой стоимости. Поиск баланса социальных и технологических факторов — долгосрочная и сложная задача, требующая комплексного подхода. Диалог с разными стейкхолдерами может внести существенный вклад в разработку стратегий, увязывающих решение социальных проблем с бизнес-целями организации.

Вопросы управления кибербезопасностью неоднократно поднимались исследователями, однако рассматривались преимущественно в контексте Индустрии 4.0. Изучались эффекты внедрения киберфизических систем для бизнеса и государственного управления (Alahmari, Duncan 2020; Kharchenko et al., 2019; Kure et al., 2018). Наша статья расширяет эти дискуссии за счет включения модели «Общества 5.0». Новые технологии — искусственный интеллект, машинное обучение, анализ данных, облачные вычисления, квантовая криптография и интернет вещей — существенно усложнили сферу кибербезопасности, и их влияние требует углубленного анализа (Sobb et al., 2020). Ожидается, что к 2025 г. оборот рынка услуг киберзащиты достигнет примерно 259 млрд долл. (Dhawan et al., 2021). Изучение потенциала возникающих технологий и его эффектов для уязвимости организаций приобрело междисциплинарный характер. Сегодня кибербезопасность охватывает такие области, как оценка и управление рисками, защита критической инфраструктуры, экономика, стратегическое планирование, инвестиционное обеспечение, информационные услуги, формирование компетенций, конкурентоспособность.

В статье предпринята попытка оценить эволюцию темы кибербезопасности и степень ее интеграции в корпоративный менеджмент.

## Методология

Наше исследование основывается на библиометрическом анализе с использованием базы Scopus — одного из наиболее обширных навигаторов по научным публикациям (Falagas et al., 2008; Mongeon, Paul-Hus, 2016). Этапы работы отражены на рис. 1. Поиск проводился в 2022 г. по ключевым словам, относящимся к двум основным темам: «кибербезопасность» и «управление». Формула поискового запроса выглядела следующим образом:

*(TITLE-ABS-KEY («cyber security*») AND TITLE-ABS-KEY (management*)) AND (LIMIT-TO (PUBSTAGE, «final»)) AND (LIMIT-TO (DOCTYPE, «ar»)) AND (LIMIT-TO (LANGUAGE, «English»)) AND (LIMIT-TO (SRCTYPE, «j»))*

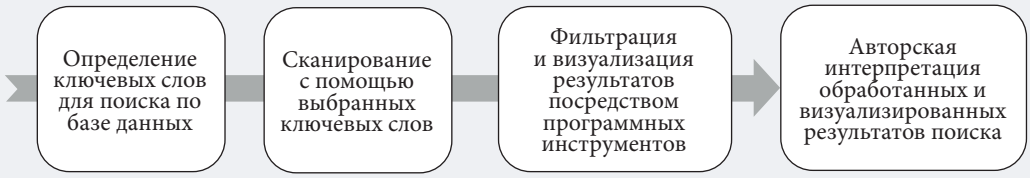
Первоначальное сканирование (до фильтрации результатов) выявило 3285 статей. Поскольку авторов интересовало только освещение в статьях аспектов менеджмента, связанных с кибербезопасностью, и учитывались публикации лишь на английском языке, на следующих стадиях список поисковых терминов корректировался. Это позволило оптимизировать выборку, которая составила 780 статей.

При установленном пороге в пять документов обнаружено одновременное употребление 314 из 5663 ключевых слов. Наряду с совместной встречаемостью понятий «кибербезопасность» и «менеджмент», анализировалась эволюция их смыслового наполнения. С помощью программы Openrefine результаты были отфильтрованы и сгруппированы на основе использования близких по смыслу терминов с разным написанием. Для визуализации данных применялись инструменты VOSviewer, R-programming и Draw. Похожие по значению слова синтезировались в единый термин (табл. 1). Оценивались частота их употребления в одних и тех же документах, эволюция исследований по рассматриваемой теме, распространенность соответствующих публикаций и масштабы совместного цитирования.

[1] Термин «киберпреступность» охватывает широкий спектр онлайн-преступлений, включая взлом информационных систем, распространение компьютерных вирусов, кражу личной информации, политических и производственных секретов, распространение дезинформации, а также попытки влиять на общественное мнение и результаты выборов. При кибератаках применяются разнообразные методы: вирусы, программы-вымогатели, социальная инженерия и др. Преступления в сети могут совершаться в рамках масштабных скоординированных операций, например, организованных государственными учреждениями или органами, спонсирующими кибератаки.

[2] https://www8.cao.go.jp/cstp/english/society5_0/index.html, дата обращения 10.07.2022.

Рис. 1. **Этапы библиометрического анализа**




*Источник*: составлено авторами.

Табл. 1. **Тезаурус для VOSviewer**

| Термин | Заменен на |
|---|---|
| Cybersecurity (кибербезопасность) | Cyber security |
| Cyber-attacks (кибератаки) | Cyber attacks |
| IoT (интернет вещей) | Internet of things (IoT) |
| Humans (люди) | human |

*Источник*: составлено авторами.

## Результаты

### *Анализ совместного употребления ключевых слов*

На рис. 2 представлены семь выявленных кластеров исследований в области кибербезопасности, обозначенных разными цветами. Термин «кибербезопасность» чаще всего встречается в желтом и красном кластерах (532 раза), как и «сетевая безопасность» (172). Данные понятия также наиболее распространены по всем кластерам (2930 и 1334 раза соответственно). Прослеживаются тесные связи двух упомянутых кластеров с другими ключевыми словами — «инвестиции», «человеческие ресурсы», «критическая инфраструктура», «информационные услуги», «принятие решений», «государственная политика», «управление рисками» и «экономика». Это свидетельствует об общем признании необходимости выстраивать унифицированные подходы к управлению кибербезопасностью для защиты критически важных инфраструктур, включая системы интернет-голосования, банковские системы и энергоснабжение (Katsikeas et al., 2021). Частая со-встречаемость пары ключевых слов «кибербезопасность» — «люди» указывает на актуальность управления человеческими ресурсами для разработки стратегий по нейтрализации киберугроз.

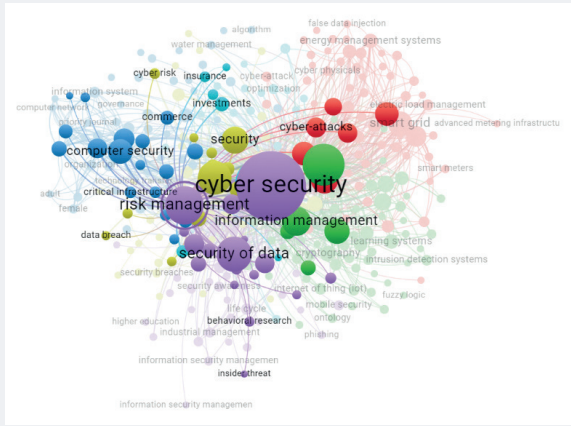
Множественные проблемы кибербезопасности не менее чем на 40% связаны с человеческим фактором, который (в случае с пользовательскими ошибками) обусловливает успех подавляющего большинства кибератак (95%). Недостаточное понимание рисков представляет серьезный вызов (Alsharif et al., 2021). Соответствующие ключевые слова также выделены авторами.

### *Эволюция темы управления кибербезопасностью*

Другая задача нашего исследования заключается в анализе тенденций совместной встречаемости ключевых слов в литературе по управлению кибербезопасностью. В основном меняется употребление терминов «компьютерная безопасность», «кибербезопасность» и «электросети» по таким направлениям, как «человеческие ресурсы», «сетевая безопасность», «автоматизация», «кибербезопасность», «информационные системы». Растет актуальность направлений: «автоматизация», «информационные системы», «сетевая безопасность», «киберугрозы», «интернет вещей», «восприятие рисков», «управление безопасностью», «распределение ресурсов» и «сложные сети» (до 203 упоминаний). Можно заключить, что динамика технологического развития влияет на освещение темы кибербезопасности (Marcantoni et al., 2022; Morgan et al., 2022).

Обсуждение вопросов киберзащиты ведется с начала 1980-х гг.[3] Первая работа из числа проиндексированных в Scopus появилась в 1999 г. «Кибербезопасность» часто употребляется в сочетании с термином «управление безопасностью», которое воспринимается организациями как инструмент снижения неопределенности и минимизации рисков (Mouti et al., 2022). Оценивая

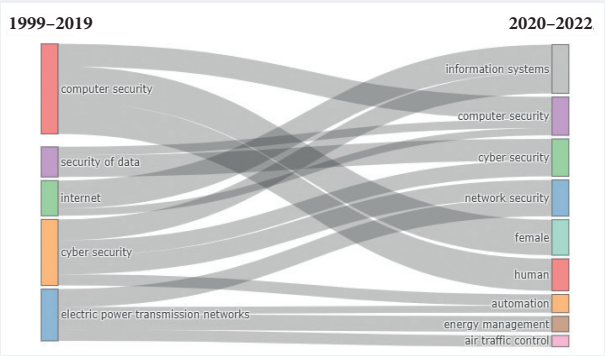
Рис. 2. **Анализ совместного употребления ключевых слов по управлению рисками**




*Источник*: составлено авторами.

[3] https://blog.avast.com/history-of-cybersecurity-avast, дата обращения 14.06.2023.

Рис. 3. **Карта тематической эволюции**




*Источник*: составлено авторами.

вероятность реализации угроз и потенциальные последствия, менеджеры по кибербезопасности получают возможность определить приоритеты для выделения ресурсов на защиту наиболее уязвимых направлений. Стратегии могут предусматривать разнообразные меры — установку брандмауэров, антивирусных приложений и систем обнаружения вторжений, составление планов превентивного реагирования на возможные инциденты и др.

На основе графиков с тремя рядами данных (рис. 3) построена «диаграмма Санки» (Sankey diagram), иллюстрирующая наиболее влиятельных авторов, организации и распространенные ключевые слова (рис. 4). Максимальное число упоминаний термина «кибербезопасность» выявлено в работах Цзи Лю (Zhi Liu), Ляньина Ванга (Lanjing Wang) и Фабио Масаччи (Fabio Masacci), которые также активно используют второе по значимости понятие «управление рисками». Среди организаций термин «кибербезопасность» чаще всего употребляется сотрудниками Университета Де Монфора (De Montfort University), о чем свидетельствует толщина потока между соответствующими полями на диаграмме. Таким образом, библиометрические данные указывают на растущее число исследований в рассматриваемом направлении. Наибольший интерес вызывают стратегии управления рисками для защиты от кибератак.

## Обсуждение

Опираясь на результаты нашего анализа и выводы предыдущих исследований, рассмотрим подробнее связь между кибербезопасностью и стратегическим управлением по таким аспектам, как инвестиции, человеческий фактор, критически важная инфраструктура, принятие решений, экономические эффекты и информационные услуги.

### *Инвестиции*

При планировании инвестиций в кибербезопасность крайне важно учитывать природу кибератак, которые могут быть как физическими, так и цифровыми (Li, Liu, 2021). В настоящее время экономическая, культурная, социальная деятельность, государственное управление и взаимодействие на всех уровнях (индивидов, неправительственных организаций, государственных органов) осуществляются преимущественно в киберпространстве микросетей (Aghajani, Ghadimi, 2018). Острота проблемы и потребность в новых компетенциях для ее решения привели к тому, что все больше компаний и национальных правительств создают специальные службы по обеспечению защиты данных. Ранее обеспечение кибербезопасности входило в функции IT-подразделений компаний и правоохранительных структур. Однако с распространением глобальных коммуникаций, международной конкуренции и геополитической напряженности на первый план выходит задача создания профильных служб на уровне государственных органов (Koputun et al., 2020)[4]. Особое внимание уделяется отслеживанию ложных новостей, прежде всего политических, распространение которых чаще всего начинается с социальных сетей. Исследования, посвященные подходам к классификации слухов и выявлению дезинформации, в последние годы демонстрируют примечательные результаты (Alsuliman et al., 2022; Isa et al., 2022).

Выделяются семь «столпов» кибербезопасности: терпение, настойчивость, защита, активность, прогнозирование, предотвращение и упреждение (Carayannis et al., 2021)[5]. Последние два из перечисленных аспектов направлены на противодействие киберугрозам и обеспечение защиты важнейших активов и систем организации, но базируются на разных подходах. Превентивные меры заключаются в выявлении уязвимостей и внедрении систем защиты, предотвращающих атаки и взлом корпоративных систем. По сравнению с ними упреждающий подход более проактивен, поскольку помогает выявлять и устранять слабые места до того, как ими воспользуются киберпреступники. Он основан на информационном мониторинге, оценке возможных угроз и тестировании на уязвимость к кибератакам. Создание комплексной системы кибербезопасности начинается с оценки текущей ситуации и потенциально уязвимых участков, далее формируется стратегия, сочетающая защитные и адаптивные меры. Ключевые этапы этого процесса приведены в табл. 2.

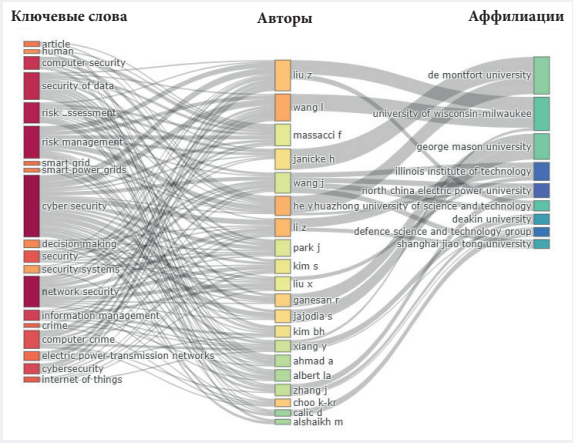
### *Человеческие ресурсы*

Связь между кибербезопасностью и человеческим капиталом становится актуальной ввиду ускоряющейся цифровизации производства и сферы услуг (Mitrofanova et al., 2017). Считается, что самым слабым звеном цепоч-

[4] В Индонезии разработку государственной политики в сфере кибербезопасности координирует Министерство связи и информационных технологий (Ministry of Communications and Information Technology, MCI). За ее реализацию отвечают Группа координации информационной безопасности (The Information Security Coordination Team), Директорат информационной безопасности (Directorate of Information Security) и Группа реагирования на инциденты безопасности в интернет-инфраструктуре (Insonesia Security Incident Response Team on Internet Infrastructure, ID-SIRTII).

[5] Оригинальные наименования терминов — patient, persistent, preserving, proactive, predictive, preventive и preemptive (7P).

**Рис. 4. Графики с тремя рядами данных**




*Источник*: составлено авторами.

**Рис. 5. Знания и навыки, необходимые специалистам по кибербезопасности**


*Источник*: составлено авторами.

ки киберзащиты являются люди, поскольку любое техническое решение по обеспечению безопасности остается под ответственностью персонала (Gratian et al., 2018). Современные профессиональные стандарты при отборе кандидатов в специалисты по кибербезопасности преимущественно уделяют внимание их академическому бэкграунду, чем общему квалификационному уровню. Как минимум они должны обладать дипломом бакалавра, предпочтительно в области информатики (Furnell, Bishop, 2020). Однако по мере развития данной сферы растет спрос на кадры, владеющие не только соответствующими технологиями, но и знаниями о культуре киберпространства, навыками сбора информации, дизайна визуальных коммуникаций, работы с материалами СМИ и др. (Pollini et al., 2022; Scanlan et al., 2020). После предварительного тестирования и приема на работу они проходят дополнительную подготовку по следующим направлениям (AlDaajeh et al., 2022; Stephanidis, Eds, 2020):

- развитие интеллектуального и ценностно-этического потенциала;
- базовые знания в области работы с информацией;
- практика сбора данных;
- мониторинг киберугроз, меры реагирования;
- аналитика, подготовка экспертных отчетов.

Управление персоналом может внести значительный вклад в обеспечение кибербезопасности путем повышения цифровой грамотности работников, разработки четких правил и процедур, обеспечения их выполнения и непосредственного участия в реагировании на инциденты.

Совокупность компетенций, которыми должны обладать специалисты по кибербезопасности, представлена на рис. 5.

**Табл. 2. Ключевые этапы разработки комплексной системы кибербезопасности**

| Мероприятие | Описание |
|---|---|
| Подготовка плана по риск-менеджменту | Выявление важнейших ресурсов и данных, оценка связанных с ними рисков, определение приоритетов для инвестирования в кибербезопасность |
| Внедрение элементов управления безопасностью | Обеспечение защиты ключевых информационных ресурсов от несанкционированного доступа посредством брандмауэров, систем контроля доступа, шифрования и др. |
| Мониторинг кибератак | Формирование систем слежения за состоянием безопасности и обнаружения вторжений |
| Формирование плана реагирования на инциденты | Ограничение масштабов киберинцидентов, смягчение последствий, ликвидация ущерба, фиксация доказательств и уведомление заинтересованных сторон |
| Составление плана восстановления системы | Восстановление данных из резервных копий, переустановка систем, внедрение новых мер безопасности для предотвращения подобных инцидентов в будущем |
| Регулярная экспертиза и обновление стратегии кибербезопасности | Оценка и корректировка стратегий кибербезопасности для выявления новых реальных и потенциальных угроз, пересмотр планов управления рисками, внедрение дополнительных мер безопасности, обучение сотрудников противодействию новым атакам |
| Разработка плана коммуникаций | Информирование заинтересованных сторон об инцидентах кибербезопасности, рисках и мерах реагирования на них, включая коммуникации с персоналом, клиентами, партнерами и регулирующими органами |

*Источник*: составлено авторами.

Табл. 3. **Меры в области кибербезопасности для защиты критических инфраструктур**

| Направление | Описание |
|---|---|
| Противодействие кибератакам | В ходе кибератак могут быть повреждены критически важные инфраструктурные системы, что вызовет масштабные сбои в их работе и поставит под угрозу безопасность отдельных людей и всего общества. Мероприятия кибербезопасности могут помочь предотвратить такие атаки путем выявления уязвимостей и принятия соответствующих мер по их исправлению |
| Обеспечение функционирования инфраструктурных систем | Для обеспечения безопасности и благополучия индивидов и сообществ критически важные инфраструктурные системы должны всегда находиться в рабочем состоянии. Меры кибербезопасности могут помочь обеспечить их нормальное функционирование и защиту от киберугроз |
| Защита конфиденциальных данных | Жизненно важные инфраструктурные системы часто содержат конфиденциальные данные, представляющие ценность для хакеров, например, личную информацию или интеллектуальную собственность. Меры кибербезопасности могут помочь защитить эту информацию от незаконного доступа и раскрытия |
| Соблюдение правил | Критически важные инфраструктурные системы подпадают под действие различных нормативных актов, в том числе Структуры кибербезопасности Национального института стандартов и технологий, в которой содержатся рекомендации по реализации мер кибербезопасности для защиты критически важных инфраструктурных систем. В случае кибератаки или другого инцидента наличие четкого плана реагирования может защитить критически важные системы и смягчить последствия |

*Источник*: составлено авторами.

### *Критическая инфраструктура*

Государственные и частные организации ежегодно тратят на технологии кибербезопасности миллионы долларов, однако они остаются уязвимыми для кибератак — как правило, потому, что рассматривают эту проблему как локальную, решаемую на внутриорганизационном уровне. Подобная ментальная установка нуждается в пересмотре, поскольку в современном мире обеспечить безопасность с помощью одних только технологий невозможно (Limba et al., 2017).

Передовые системы управления производственными процессами состоят из компьютерных устройств, датчиков контроля и сетевого оборудования для дистанционного регулирования жизненно важных инфраструктур (водо- и энергоснабжение, транспорт и др.). Отключение этих систем в результате кибератак приведет к остановке производства, создаст угрозу безопасности людей, окружающей среды и др. (Catota et al., 2019; Firoozjaei et al., 2022). Исключить подобные сценарии может специальная инфраструктура, особенно в отношении киберфизических систем (de Soto et al., 2022), однако задача ее создания осложняется ввиду разнородности используемых устройств, протоколов и повышенных требований к их надежности (Michalec et al., 2022).

Наращиванию потенциала национальной кибербезопасности будет способствовать расширение сети специализированных учебных центров и аналитических лабораторий (Qi et al., 2018; Quincozes et al., 2022) в формате государственно-частного партнерства. Устройство подобной инфраструктуры будет зависеть от того, как государство и бизнес понимают свою роль в ее укреплении. Зачастую взаимные ожидания сторон в данной области не соответствуют друг другу (Carr, 2016; Watanabe, 2019). Национальная инфраструктура кибербезопасности должна носить комплексный характер, поскольку физические и цифровые функциональные системы (электросети, транспортные системы, системы водоснабжения, сети коммуникаций и др.) тесно взаимозависимы, поэтому нарушения в одной могут иметь серьезные последствия для других. В табл. 3 приведены примеры шагов по защите критической инфраструктуры.

### *Информационные услуги*

Информационные сервисы предоставляют сведения разным категориям пользователей, но их недостаточная осведомленность о киберрисках может привести к утечке важных персональных и корпоративных данных. Несмотря на то что современные программные алгоритмы способны самостоятельно выявлять некоторые фишинговые электронные письма и сайты, они не гарантируют абсолютной надежности, учитывая растущее применение киберпреступниками методов социальной инженерии (Mantha, de Soto, 2021). Решением видятся интенсивное информирование пользователей о подобных факторах риска (Rajan et al., 2021) и ужесточение политики по соблюдению конфиденциальности.

### *Принятие решений*

В настоящее время рассматривается возможность использования искусственного интеллекта для принятия решений в области кибербезопасности (Zyoud, Fuchs-Hanusch, 2017). Подобные технологии помогают аккумулировать и перерабатывать колоссальные массивы данных о потенциальных киберугрозах с использованием поведенческой теории принятия решений. На этой основе эксперты расставляют приоритеты реагирования. Последовательность обработки и фильтрации информации в отношении кибербезопасности с применением искусственного интеллекта представлена в табл. 4.

### *Управление рисками*

Кибербезопасность тесно связана с оценкой и управлением рисками — необходимой деятельностью для создания критической инфраструктуры и поддержки в принятии решений. При планировании соответствующей инфраструктуры кибербезопасности учитываются более широкие задачи разных уровней, включая поддержку экономического роста, реализацию организационных целей, обучение персонала и др. Методы анализа рисков широко применяются для прогнозирования будущих событий (Kure et al., 2018; Michalec et al., 2022; Mitrofanova et al., 2017; Rosado et al., 2022). Состояние системы кибербезопасности стало одним из ключевых индикаторов уровня развития страны наряду

Табл. 4. **Меры в области кибербезопасности для защиты критических инфраструктур**

| Этап | Описание |
|---|---|
| Сбор данных | Аналитическая служба получает информацию двух типов: из открытых источников (социальные сети, СМИ и т.п.), и закрытые данные от агентов (Hautamaki, Kokkonen, 2020). Сведения должны быть оперативными, точными и достоверными. |
| Программная обработка | Собранная информация обрабатывается искусственным интеллектом. |
| Экспертные заключения | Рекомендации искусственного интеллекта рассматриваются и фильтруются экспертами, после чего принимается окончательное решение. |
| Оценка ситуации | Предприятия изучают обстановку на предмет киберугроз и их последствий (Jiang et al., 2022). В экстренных случаях решение принимает руководитель службы по работе с информацией. Если оперативного реагирования не требуется, либо достоверность и полнота сведений вызывают сомнения, они уточняются путем прохождения всех регламентных процедур. |

Источник: составлено авторами.

с классическими показателями (ВВП и т. п.). Получило развитие новое направление — «экономика кибербезопасности», оценивающее риски и преимущества для различных игроков (индивидов, организаций, государств) с точки зрения потенциальных киберугроз, их поведенческие паттерны, стратегии, а также влияние государственного регулирования и рыночных механизмов на состояние кибербезопасности (Jentzsch, 2018). В отношении национальной безопасности превентивная оценка рисков поможет минимизировать угрозы, исходящие из таких источников, как международные конфликты, политические протесты, торговля инсайдерской информацией, атаки с помощью вредоносных программ, шпионаж и др. (McEvoy, Kowalski, 2019). Для анализа и устранения этих факторов используются разные методологии управления рисками[6]. Они заслуживают более подробного анализа в ходе дальнейших эмпирических исследований в области управления кибербезопасностью.

## Заключение

С динамичным развитием и повсеместным проникновением технологий, прежде всего информационных и коммуникационных, актуализируется проблема кибербезопасности, имеющая стратегическое значение, а в последние годы получившая еще и юридическое измерение. Защищенность активов, данных и репутации от все более частых и изощренных кибератак определяется умением разрабатывать и постоянно обновлять комплексный, упреждающий подход к кибербезопасности, охватывающий кадровые, процедурные и технологические аспекты.

В статье проанализированы тенденции эволюции исследований по теме кибербезопасности и ее связь с ключевыми аспектами стратегического корпоративного менеджмента, включая инвестиции в инфраструктуру и человеческий капитал. Ключевым аспектом обеспечения кибербезопасности остается работа с людьми как наиболее уязвимым звеном в цепочке. Основные направления мер включают подготовку специалистов по кибербезопасности с широким набором универсальных компетенций и информирование рядовых пользователей о потенциальных киберугрозах.

Соблюдение кибербезопасности требует регулярного мониторинга данных, оценки рисков, превентивного выявления слабых мест и разработки мер по их устранению. Непрерывность этого процесса достигается легче, а эффективность повышается, если создана гибкая организационная система, координирующая взаимодействие между разными подразделениями.

Представленное исследование имеет свои ограничения, поскольку освещает вопросы кибербезопасности лишь в глобальном обобщенном измерении. Анализировалась только литература на английском языке как наиболее распространенном в научной коммуникации. В ходе дальнейших исследований рекомендуется рассмотреть более широкий контекст стратегического управления кибербезопасностью, чтобы получить более полное представление о текущей ситуации.

*Авторы заявляют об отсутствии конфликта интересов. Данные, использованные для выполнения настоящего исследования, доступны через базу данных Scopus. При наличии авторизованного доступа к этой базе данных никакого дополнительного разрешения не требуется. Не требуется также информированного согласия авторов использованных в настоящем исследовании материалов, поскольку оно представляет собой обзор литературы.*

## Библиография

Aghajani G., Ghadimi N. (2018) Multi-Objective Energy Management in a Micro-Grid. *Energy Reports,* 4, 218–225. https://doi.org/1010.1016/j.egyr.2017.10.002

Alahmari A., Duncan B. (2020) *Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence*. Paper presented at the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020, 15-19 June 2020, Dublin, Ireland). https://doi.org/10.1109/CyberSA49311.2020.9139638

[6] Например, CRAMM (CCTA Risk Analysis and Management Method), OCTAVE Allegro, Infosec Standard 1, FAIR (Factor Analysis of Information Risk), MEHARI (MEthod for Harmonized Analysis of RIsk), STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege), SABSA (Risk), Attack Path Analysis, IRAM (Information Risk Assessment Methodology).

AlDaajeh S., Saleous H., Alrabaee S., Barka E., Breitinger F., Choo K.K.R. (2022) The Role of National Cybersecurity Strategies on the Improvement of Cybersecurity Education. *Computers and Security,* 119, 102754. https://doi.org/10.1016/j.cose.2022.102754

Alsharif M., Mishra S., AlShehri M. (2021) Impact of Human Vulnerabilities on Cybersecurity. *Computer Systems Science and Engineering,* 40(3), 1153–66. https://doi.org/10.32604/CSSE.2022.019938

Alsuliman F., Bhattacharyya S., Slhoub K., Nur N., Chambers C.N. (2022) Social Media vs. News Platforms: A Cross-Analysis for Fake News Detection Using Web Scraping and NLP. In: *PETRA'22: Proceedings of the 15th International Conference on PErvasive Technologies Related to Assistive Environments,* June 2022, pp. 190–196. https://doi.org/10.1145/3529190.3534755

Amir M., Givargis T. (2020) Pareto Optimal Design Space Exploration of Cyber-Physical Systems. *Internet of Things,*12, 100308. https://doi.org/10.1016/j.iot.2020.100308

Carayannis E.G., Grigoroudis E., Rehman S.S., Samarakoon N. (2021) Ambidextrous Cybersecurity: The Seven Pillars (7Ps) of Cyber Resilience. *IEEE Transactions on Engineering Management,* 68(1), 223–34. https://doi.org/10.1109/TEM.2019.2909909

Carr M. (2016) Public Private Partnerships in India. *International Affairs,* 92(1), 43–62.

Catota F.E., Granger M.M., Sicker D.C. (2019) Cybersecurity Education in a Developing Nation: The Ecuadorian Environment. *Journal of Cybersecurity,* 5(1), 1–19. https://doi.org/10.1093/cybsec/tyz001

De Soto B.G., Georgescu A., Mantha B., Turk Z., Maciel A., Sonkor S.M. (2022) Construction Cybersecurity and Critical Infrastructure Protection: New Horizons for Construction 4.0. *Journal of Information Technology in Construction,* 27, 571–594. https://doi.org/10.36680/j.itcon.2022.028

Dhawan S.M., Gupta B.M., Elango B. (2021) Global Cyber Security Research Output (1998–2019): A Scientometric Analysis. *Science and Technology Libraries,* 40(2), 172–189. https://doi.org/10.1080/0194262X.2020.1840487

Falagas M.E., Pitsouni E.I., Malietzis G.A., Pappas G. (2008) Comparison of PubMed, Scopus, Web of Science, and Google Scholar: Strengths and Weaknesses. *The FASEB Journal,* 22(2), 338–342. https://doi.org/10.1096/fj.07-9492lsf

Firoozjaei M.D., Mahmoudyar N., Baseri Y., Ghorbani A.A. (2022) An Evaluation Framework for Industrial Control System Cyber Incidents. *International Journal of Critical Infrastructure Protection,* 36(C), 100487. https://doi.org/10.1016/j.ijcip.2021.100487

Furnell S., Bishop M. (2020) Addressing Cyber Security Skills: The Spectrum, Not the Silo. *Computer Fraud and Security,* 2020(2), 6–11. https://doi.org/10.1016/S1361-3723(20)30017-8

Gratian M., Bandi S., Cukier M., Dykstra J., Ginther A. (2018) Correlating Human Traits and Cyber Security Behavior Intentions. *Computers and Security,* 73, 345–358. https://doi.org/10.1016/j.cose.2017.11.015

Härtel J.C.R., Härtel C.E.J. (2022) What the Digital Age Is and Means for Workers, Services, and Emotions Scholars and Practitioners. *Research on Emotion in Organizations,* 16, 9–17. https://doi.org/10.1108/S1746-979120200000016003

Hautamaki J., Kokkonen T. (2020) *Model for Cyber Security Information Sharing in Healthcare Sector.* Paper presented at the 2nd International Conference on Electrical, Communication and Computer Engineering, ICECCE 2020, June 12–13, Istanbul, Turkey. https://doi.org/10.1109/ICECCE49384.2020.9179175

Isa S.M., Nico G., Permana M. (2022) Indobert for Indonesian Fake News Detection. *ICIC Express Letters,* 16(3), 289–297. https://doi.org/10.24507/icicel.16.03.289

Jentzsch N. (2018) *State-of-the-Art of the Economics of Cyber-Security and Privacy* (IPACSO Deliverable D4.1). https://doi.org/10.2139/ssrn.2671291

Jiang L., Jayatilaka A., Nasim M., Grobler M., Zahedi M., Ali Babar M. (2022) Systematic Literature Review on Cyber Situational Awareness Visualizations. *IEEE Access,* 10, 57525–57554. https://doi.org/10.1109/access.2022.3178195

Katsikeas S., Johnson P., Ekstedt M., Lagerström R. (2021) Research Communities in Cyber Security: A Comprehensive Literature Review. *Computer Science Review,* 42, 100431. https://doi.org/10.1016/j.cosrev.2021.100431

Kharchenko V., Dotsenko S., Illiashenko O., Kamenskyi S. (2019) Integrated Cyber Safety Security Management System: Industry 4.0 Issue. In: *Conference Proceedings of 2019 10th International Conference on Dependable Systems, Services and Technologies, DESSERT 2019*, June 5–7, pp. 197–201. https://doi.org/10.1109/DESSERT.2019.8770010

Kopotun I., Nikitin A., Dombrovan N., Tulinov V., Kyslenko D. (2020) Expanding the Potential of the Preventive and Law Enforcement Function of the Security Police in Combating Cybercrime in Ukraine and the EU. *TEM Journal,* 9(2), 460–468. https://doi.org/10.18421/TEM92-06

Kure H.I., Islam S., Abdur Razzaque M. (2018) An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. *Applied Sciences (Switzerland),* 8(6), 8060898. https://doi.org/10.3390/app8060898

Li Y., Liu Q. (2021) A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments. *Energy Reports,* 7, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Limba T., Plėta T., Agafonov K., Damkus M. (2017) Cyber security management model for critical infrastructure. *Entrepreneurship and Sustainability Issues*, 4(4), 559–573. http://dx.doi.org/10.9770/jesi.2017.4.4(12)

Mantha B.R.K., de Soto B.G. (2021) Assessment of the Cybersecurity Vulnerability of Construction Networks. *Engineering, Construction and Architectural Management,* 28(10), 3078–3105. https://doi.org/10.1108/ECAM-06-2020-0400

Marcantoni M., Jayawardhana B., Perez Chaher M., Bunte K. (2022) Secure Formation Control via Edge Computing Enabled by Fully Homomorphic Encryption and Mixed Uniform-Logarithmic Quantization. *IEEE Control Systems Letters*, 7, 395–400. https://doi.org/10.1109/LCSYS.2022.3188944

McEvoy R., Kowalski S. (2019) Cassandra's Calling Card: Socio-Technical Risk Analysis and Management in Cyber Security Systems. In: *CEUR Workshop Proceedings,* vol. 2398, pp. 65–80.

Michalec O., Milyaeva S., Rashid A. (2022) When the Future Meets the Past: Can Safety and Cyber Security Coexist in Modern Critical Infrastructures? *Big Data & Society,* 9(1), 205395172211083. https://doi.org/10.1177/20539517221108369

Mitrofanova A., Konovalova V., Mitrofanova E., Ashurbekov R., Trubitsyn T. (2017) *Human Resource Risk Management in Organization: Methodological Aspect*. Paper presented at the International Conference on Trends of Technologies and Innovations in Economic and Social Studies 2017. https://doi.org/10.2991/ttiess-17.2017.114

Mongeon P., Paul-Hus A. (2016) The Journal Coverage of Web of Science and Scopus: A Comparative Analysis. *Scientometrics,* 106(1), 213–228. https://doi.org/10.1007/s11192-015-1765-5

Morgan P.L., Collins E.I.M., Spiliotopoulos T., Greeno D.J,, Jones D.M. (2022) Reducing Risk to Security and Privacy in the Selection of Trigger-Action Rules: Implicit vs. Explicit Priming for Domestic Smart Devices. *International Journal of Human – Computer Studies,* 168, 102902. https://doi.org/10.1016/j.ijhcs.2022.102902

Mouti S., Kumar S., Althubiti S.A., Altaf M., Alenezi F., Arumugam M. (2022) Cyber Security Risk Management with Attack Detection Frameworks Using Multi Connect Variational Auto-Encoder with Probabilistic Bayesian Networks. *Computers and Electrical Engineering,* 103, 108308. https://doi.org/10.1016/j.compeleceng.2022.108308

Pollini A., Callari T.C., Tedeschi A., Ruscio D., Save L., Chiarugi F., Guerri D. (2022) Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach. *Cognition, Technology and Work,* 24(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

Qi A., Shao G., Zheng W. (2018) Assessing China's Cybersecurity Law. *Computer Law and Security Review,* 34(6),1342–1354. https://doi.org/10.1016/j.clsr.2018.08.007

Quincozes S.E., Mosse D., Passos D., Albuquerque C., Ochi L.S., Dos Santos V.F. (2022) On the Performance of GRASP-Based Feature Selection for CPS Intrusion Detection. *IEEE Transactions on Network and Service Management,* 19(1), 614–626. https://doi.org/10.1109/TNSM.2021.3088763

Rajan R., Rana N.P., Parameswar N., Dhir S., Sushil S., Dwivedi Y.K. (2021) Developing a Modified Total Interpretive Structural Model (M-TISM) for Organizational Strategic Cybersecurity Management. *Technological Forecasting and Social Change,* 170, 120872. https://doi.org/10.1016/j.techfore.2021.120872

Rosado D.G., Santos-Olmo A., Sánchez L.E., Serrano M.A., Blanco C., Mouratidis H., Fernández-Medina E. (2022) Managing Cybersecurity Risks of Cyber-Physical Systems: The MARISMA-CPS Pattern. *Computers in Industry,* 142, 103715. https://doi.org/10.1016/j.compind.2022.103715

Scanlan J., Thomas T., Tan T., Chen Y.P., Watters P.A., Fieldhouse M., Fung L., Girdler S. (2020) *Neurodiverse Knowledge, Skills and Ability Assessment for Cyber Security*. Paper presented at the Australasian Conference on Information Systems 2020, Wellington. https://www.researchgate.net/publication/350964865_Neurodiverse_Knowledge_Skills_and_Ability_Assessment_for_Cyber_Security, дата обращения 19.04.2023.

Sobb T., Turnbull B., Moustafa N. (2020) Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions. *Electronics (Switzerland),* 9(11), 9111864. https://doi.org/10.3390/electronics9111864

Watanabe K. (2019) PPP (Public-Private Partnership)-Based Cyber Resilience Enhancement Efforts for National Critical Infrastructures Protection in Japan. In: *Critical Information Infrastructures Security* (Proceedings of the 13th International Conference, CRITIS 2018, Kaunas, Lithuania, September 24-26, 2018), Heidelberg, Dordrecht, London, New York: Springer, pp. 169–178. https://doi.org/10.1007/978-3-030-05849-4_13

Zyoud H., Fuchs-Hanusch D. (2017) A bibliometric-based survey on AHP and TOPSIS techniques. *Expert Systems with Applications*, 78, 158–181. https://doi.org/10.1016/j.eswa.2017.02.016