КИБЕРБЕЗОПАСНОСТЬ: ОСНОВНЫЕ ТЕНДЕНЦИИ В ОБЕСПЕЧЕНИИ

Ловцов Д.А.[1], Бурый А.С.[2]

Ключевые слова: *кибербезопасность, компьютерные системы, критическая информационная инфраструктура, критически важные объекты, информационно-коммуникационные технологии, информационное пространство, кибератаки, киберсфера, стандартизация, киберустойчивость, информационная надежность, информационная добротность, проблема.*

Аннотация

Цель работы: совершенствование научной и методической базы теории защищенности информации и информационной безопасности критически важных объектов.

Методы: системный и экспертный анализ, концептуально-логическое моделирование, формально-логическая разработка и обоснование математической структуры проблемы стратегической киберустойчивости.

Результаты: дана общая характеристика кибербезопасности как свойства компьютерных систем; рассмотрены основные понятия и определения, тенденции и подходы в обеспечении кибербезопасности в России и в Североатлантическом альянсе; определены возможности стандартизации киберсферы; определены цели и задачи обеспечения киберустойчивости как целевого фактора, ориентированного на кибербезопасность; обоснованы частные численные показатели и критерии киберустойчивости; обоснована математическая структура и предложен путь решения проблемы стратегической устойчивости в области коллективной кибербезопасности; даны общие рекомендации по обеспечению киберзащиты в стратегических сетевых операциях.

DOI: 10.21681/1994-1404-2024-2-23-34

Введение

Успех современных специальных информационно-ударных операций [6] (включая сетевые) во многом определяется *информационно-коммуникационными технологиями* (ИКТ), которые, в свою очередь, диктуют направления совершенствования систем вооружения, военной и специальной техники и, как следствие, стратегий ведения боевых действий. При этом используемые *компьютерные системы* (управляющие вычислительные комплексы, автоматизированные системы управления боевыми средствами и др.) критически важных объектов (КВО) находятся под угрозой как со стороны целенаправленных сетевых атак хакеров, так и обычных компьютерных и сетевых вирусов.

Начало XXI в. ознаменовалось формированием новой — *цифровой* реальности, которая, наряду с очевидным улучшением качества жизни человечества, существенно сузила пространство безопасности *информационной инфраструктуры* [11, 12]. Комплекс качественно новых угроз и вызовов (включая *кибератаки, киберпреступления, кибертерроризм, кибердиверсии, кибервойны* и др.) поставил в международную повестку вопрос об объединении усилий многих стран в деле обеспечения надежной защиты *цифровой среды* (*киберсреды* [22]), как внутренней, так и глобальной [3].

В частности, институциональной политикой стран-участниц блока НАТО стало обеспечение *кибербезопасности* как свойства компьютерных систем, характеризующего степень их защищенности от *кибератак* — попыток нарушить работу, заблокировать или уничтожить компьютеры, их сети, сети сотовой связи, цифровые медиа, региональные и глобальные телематические сети (ГТС), причем осуществляемых как по традиционным, так и по *нетрадиционным* (скрытым) информационным каналам [11, 14]. То есть кибербе-

[1] ***Ловцов Дмитрий Анатольевич***, *доктор технических наук, профессор, заслуженный деятель науки Российской Федерации, заместитель по научной работе директора Института точной механики и вычислительной техники им. С. А. Лебедева Российской академии наук, заведующий кафедрой информационного права, информатики и математики Российского государственного университета правосудия, г. Москва, Российская Федерация.*

E-mail: dal-1206@mail.ru

[2] ***Бурый Алексей Сергеевич***, *доктор технических наук, директор департамента Российского института стандартизации, ведущий научный сотрудник Института проблем управления им. В. А. Трапезникова Российской академии наук, г. Москва, Российская Федерация.*

E-mail: a.s.burij@gostinfo.ru

зопасность отражает элементы безопасности в виртуальном мире ГТС (типа Интернет, Релком, Ситек, *Sedab*, *Remart* и др.) [24].

Если на первых порах целями киберпреступлений становились промышленные объекты, инновационные технологии [21], то теперь, помимо «естественного фона» — интереса к вопросам оборонно-промышленного комплекса [2] и КВО [4] — злоумышленники все чаще рассматривают социальные объекты как потенциальные мишени своего воздействия [19], например, *биометрические технологии* в процессах взаимодействия «банк — клиент» (в ходе идентификации и подтверждения финансовых операций клиентами) [8].

За сравнительно небольшое время обеспечение кибербезопасности из отдельного направления обеспечения *информационной безопасности* [11] всё больше заявляет о себе как о междисциплинарной предметной области, занимающей промежуточное положение между сферой ИКТ и сферами других предметных областей — от безопасности до бизнеса, предпринимательства, правоприменения и др.

В этой связи требуют решения вопросы разработки концепции проблемно-ориентированного *комплексного подхода* [10] к обеспечению кибербезопасности, включая разработку методологии и инструментария для практического внедрения, образовательный сегмент, возможности искусственного интеллекта, реализованные в отечественных аппаратно-программных средах, и др. [17].

Варианты «сдерживания» в киберпространстве

В западных источниках все активнее даются прогнозы на использование *кибероружия* в будущих вооруженных столкновениях[3] [25]. Эти наступательные кибернетические возможности в руках противников представляют значительную угрозу вооруженным силам и КВО для каждой из сторон конфликта. Североатлантический альянс (НАТО) признает, что кибератаки (как гибридные угрозы) могут быть такими же разрушительными, как и обычные военные действия. Вредоносные кибератаки, нацеленные на такие компьютерные системы, как *управляющие вычислительные комплексы* КВО, могут быть не менее опасными, чем угрозы физического характера, и могут привести к взрывам, ядерным авариям, отключениям электроэнергии или финансовым кризисам. По заявлениям представителей НАТО, *«всего за несколько минут одна кибератака может нанести ущерб экономике на миллиарды долларов, парализовать критическую информационную инфраструктуру и подорвать военный потенциал»*[4].

В рассуждениях западных военных кибераналитиков прослеживается идея необходимости развития наступательных кибервозможностей и интеграции их в военные операции. Для того чтобы избежать перерастания в тотальную войну ситуации «*тумана войны*» (термин обозначает отсутствие *достоверной* информации о текущей обстановке), союзники по Альянсу должны согласовать перечень гибких средств «сдерживания», которые позволят постепенно наращивать давление в *киберпространстве* [23] для ограничения масштаба и интенсивности возможных конфликтов, хотя нет гарантий, что эти меры могут быть использованы в качестве превентивных.

Гибкие варианты «сдерживания» НАТО в киберпространстве могли бы включать следующие действия (рис. 1)[5]:

(1) повышение готовности сил и средств посредством киберобразования, тренингов и учений;

(2) развертывание групп «быстрого реагирования» в киберпространстве для проведения оборонительных кибероперациий и защиты КВО;

(3) повышение информированности общественности о вредоносной кибердеятельности и потенциальном конфликте в киберпространстве;

(4) принятие мер по взаимной поддержке союзных государств Альянса;

(5) расширение мер по информационному взаимодействию в киберпространстве;

(6) официальные заявления о нарушениях международного права в киберпространстве;

(7) приведение в готовность и развертывание сил для проведения наступательных кибероперациий;

(8) введение киберсанкций;

(9) проведение наступательных кибероперациий для достижения эффекта *A2/AD* (препятствие доступу/закрытию зоны — *Anti-Access/Area Denial*) в киберпространстве;

(10) приведение комплекса мер в соответствии с Договором Альянса в полной мере;

(12) проведение наступательных кибероперациий совместно с другими маневренными силами во всем оперативном пространстве.

Характеристика состояния кибербезопасности

В эпоху активного использования возможностей ГТС все ещё не удаётся обеспечить надежную защиту от *кибермошенничества* [5]. В «Лаборатории Касперского» проанализирована статистика переходов по заблокированным фишинговым[6] ссылкам[7] и составлен рей-

[3] Iftimie I.A. NATO's needed offensive cyber capabilities. NATO Defense College. 2020. URL: http://www.jstor.org/stable/resrep25100 (дата обращения: 29.02.24).

[4] Там же.

[5] Там же.

[6] *Фишинг* (от англ. *fishing* — рыбачить, выуживать) — разновидность попыток несанкционированного доступа, когда жертву провоцируют на разглашение информации, посылая ей фальсифицированное электронное письмо с приглашением посетить веб-сайт, который на первый взгляд связан с законным источником.

[7] ГОСТ Р 56205-2014. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели. М. : Стандартинформ, 2020. 76 с.

Рис. 1. Гибридные варианты «сдерживания» в киберпространстве

тинг ресурсов, которые подделывают чаще всего. На *первом* месте — мессенджеры (19%), *второе* место занимают почтовые сервисы и веб-порталы (18,5%), *третьими* в списке оказались онлайн-игры — 11%, затем идут банки — 10,5% и на *пятом* месте — онлайн-магазины с 8%[8]. *Киберпреступность* становится целевой деятельностью формирующегося «бизнес-сообщества» со своими правилами и конкуренцией, которая постоянно совершенствуется для привлечения новых клиентов-преступников и, соответственно, денег. Разумеется, это не означает, что пользователям следует отказаться от онлайн-сервисов, так как средства обеспечения кибербезопасности находятся в постоянной готовности к локализации новых и усовершенствованных старых угроз, но вместе с тем следует уделять должное внимание этому вопросу, иначе однажды можно безнадежно отстать.

Кибербезопасность — это важная цель стратегий, как превентивных, так и/или упреждающих действий, обеспечивающих технологический рост и продвижение вперед, базирующихся на инновациях, так как надо научиться быть всегда на шаг впереди возможных действий другой (конкурирующей или противоборствующей) стороны. Реальности виртуального *информационного пространства* [11, 12], которую нам обеспечивает Всемирная паутина, существующие информационные методы и возможности пронизывают в настоящее время все стороны жизни, полностью или частично определяя множество современных ИКТ. Все соответствующие инструменты, с которыми работают профессионалы или частные лица в определенные моменты времени, зависят от технологических достижений, облегчающих и одновременно усложняющих их жизнедеятельность. Вместе с тем *информационные деятели* (пользователи, операторы, авторы и др.) нуждаются в постоянной и надежной кибербезопасности своих данных, а также виртуального «образа жизни»[9].

В частности, динамика дальнейшего развития кибервозможностей стран НАТО имеет многовекторный характер и тенденцию развития многопрофильности кибероборонь Альянса[10]. Надо понимать, что вместе с активным внедрением ИКТ неизбежно будет расти и уязвимость защитных мер, и дополнительные расходы на оборону. Предусмотреть, изучить и предотвратить различные виды кибератак намного сложнее, чем реагировать на традиционные типы угроз [7]. Поэтому в ответ на действия зарубежных поставщиков Президентом РФ принято решение о развитии программы импортозамещения и установлен срок перехода на отечественные средства киберзащиты — до 1 января 2025 г. Среди прочего вводится запрет на использование любого иностранного программного обеспечения на объектах *критической информационной инфраструктуры* (КИИ) России[11]. Поэтому в настоящее время осуществляется замена в государственных организациях и компаниях операционной системы *Microsoft Windows* на отечественную операционную систему *Astra Linux*[12].

[8] Киберпреступность: основные тренды и угрозы в 2024 г. URL: https://realnoevremya.ru/articles/303048-kiberprestupnost-osnovnye-trendy-i-ugrozy-v-2024-godu (дата обращения: 29.02.2024).

[9] Efthymiopoulos M. P. A cyber-security framework for development, defense and innovation at NATO // Journal of Innovation and Entrepreneurship. 2019. Т. 8. № 1.

[10] *См., например,* Стратегию национальной кибербезопасности США 2018 г.: National Cyber Strategy of the United States of America 2018. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения: 29.02.2024).

[11] Указ Президента Российской Федерации от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации». URL: http://publication.pravo.gov.ru/Document/View/0001202203300001?index= 2 (дата обращения: 29.02.24).

[12] URL: https://ru.m.wikipedia.org/wiki/Astra_Linux (дата обращения: 29.02.24).

Таблица 1

Основные понятия и определения в области кибербезопасности

Понятия и прикладные определения	Источники
Кибербезопасность (киберзащита) — действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли, или повреждения критических систем или информационных объектов. Кибербезопасность включает в себя понятия идентификации, аутентификации, отслеживаемости, авторизации, доступности и приватности.	ГОСТ Р 56205-2014 (п. 3.2.36)
Информационная безопасность — сохранение конфиденциальности, целостности и возможности доступа к информации. *Безопасность информации* [данных] определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, с несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые при применении информационной технологии.	ГОСТ Р 57392-2017 (п. 2.11); Р 50.1.056-2005 (п. 3.1.3)
Компьютерная безопасность — защита компьютерного аппаратного и программного обеспечения от случайного или предумышленного доступа, использования, модификации, уничтожения или разглашения. Безопасность относится также к персоналу, данным, коммуникационным связям и физической и логической защите компьютерных инсталляций.	ГОСТ 33647-2015 (п. 3.5.10)
Киберпространство — это зависящий от времени набор материальных и нематериальных активов, которые хранят и/или передают электронную информацию.	Kutlu F.B. [26]
Кибератака — все возможные вредоносные действия, направленные на нарушение целостности, доступности и конфиденциальности информационных сетей, систем или непосредственно информации.	Jasper S. [25]
Компрометация данных — нарушение безопасности, которое приводит к случайному или незаконному разрушению, потере, изменению, несанкционированному раскрытию или доступу к защищаемым данным, передаваемым, хранимым или иным образом обрабатываемым.	ГОСТ Р ИСО/МЭК 27017-2021 (п. 3.1.2)

Наблюдая достаточно активное развитие базовых компонентов *киберсферы* (*цифровой сферы* [11]), т. е. *киберсреды* [22] как материальной области киберсферы и *киберпространства* как соответствующей виртуальной области в части создания и применения новых методов и способов несанкционированного проникновения в компьютерные системы, с *одной стороны*, а также эффективных средств защиты привилегированных данных, с *другой стороны*, — пока всё ещё рано говорить о едином подходе к формированию терминологической системы в данной предметной области. Поэтому до сих пор нет соответствующих общепринятых определений.

В табл. 1 представлен ряд *прикладных* определений, как на основе действующих стандартов, так и с учетом данных Европейского агентства сетевой и информационной безопасности (*European Union Agency for Cybersecurity*)[13] [26]. Из табл. 1 видно, что кибербезопасность рассматривается сегодня как широкое понятие, и поэтому представляется целесообразным выявлять различия между возможными типами кибератак.

Например, *киберпреступность* является растущей сферой противоправной деятельности, поэтому следует своевременно совершенствовать меры нормативно-правового характера. То есть на современном этапе определяющую роль в борьбе с киберпреступностью играют органы государственного управления и органы правосудия. Вместе с тем *кибершпионаж* — это та область, где задачи, решаемые военными органами, представляют интерес для эвентуального противника, поскольку отраслевые сети и объекты соответствующих предприятий и научных центров хранят чрезвычайно важную конфиденциальную информацию, которая может быть использована в политических и военных интересах многих стран.

Кибертерроризм, кибердиверсии, кибервойны и др., а также возможные результаты соответствующей деструктивной деятельности представляют серьезную опасность для КИИ (включая программное обеспечение, системы управления, средства связи и информационные сети госструктур, банков, предприятий топливно-энергетического комплекса и др.) КВО, повреждение компонентов которой может привести к серьёзным последствиям для экономики и населения. Силы Альянса, например, участвовали в широком спектре конфликтов после окончания «холодной войны», и *кибероперации* все чаще становятся частью этих конфликтов и элементом планов и сценариев военных действий.

В табл. 2 представлены категории многомерных проблем, связанных с обеспечением кибербезопасности, и указаны области, в которых участники Североатлантического альянса могут иметь основные интересы [24].

[13] Iftimie I.A. NATO's needed offensive cyber capabilities // NATO Defense College. 2020. URL: http://www.jstor.org/stable/resrep25100 (дата обращения: 29.02.2024).

Таблица 2

Кибербезопасность в отношении целей, категорий и мотивации

Целевые объекты кибератак	**Киберпреступность** (преступная мотивация)	**Кибершпионаж** (расширение возможностей государства)	**Кибертерроризм** (политическое принуждение, вызывающее страх)	**Кибервойна** (усиление вооруженных операций)
Частные лица	+			
Предприятия КИИ	+	+	+	+
Предприятия не из состава КИИ	+	+	+	+
Правительственные ведомства/ объекты		+	+	+
Вооруженные силы / силы обороны		+	+	+
Условные обозначения: — основная роль НАТО; — периферийная роль НАТО.				

Идеи стандартизации киберсферы

Киберсфера как сложная эргатическая система объединяет в себе самих информационных деятелей (источников и потребителей информации), сетевую инфраструктуру, аппаратное и программное обеспечение, процессы и сервисы, локальную, облачную или транзитную информацию, включая системные носители информации, которые можно подключить прямо или косвенно к ГТС. Одной из ключевых задач данной эргасистемы является обеспечение её кибербезопасности путем снижения риска сбоев и отказов функционирования, включая предотвращение или смягчение последствий кибератак.

Способность многих стран работать сообща в новых условиях кибербезопасности важна как никогда. На межгосударственном уровне целесообразно использовать общий набор стандартов в сферах торговли, информационного обмена, образования и др. Этому способствуют, в частности, существующие отечественные *системы классификации и кодификации*[14] [16].

Например, стандартизация *киберсферы* Североатлантического альянса направлена на разработку и внедрение соответствующих концепций, доктрин и процедур для достижения и поддержания требуемых уровней *совместимости*, *взаимозаменяемости* и *общности* компьютерных систем, необходимых для достижения *интероперабельности*[15] как способности двух или более компьютерных систем к обмену и использованию информации.

Совместимость обеспечивает возможность встраиваться в компьютерную (информационную) систему с другим типом оборудования (например, в случае венгерских сил обороны — с российским оборудованием[16]). *Взаимозаменяемость* дает возможность обмена одного оборудования на другое. В ходе совместных операций страны могут обмениваться всеми типами ресурсов. *Общность* выражает состояние, при котором различные группы используют общие ресурсы или преследуют общие цели за счет реализации интеграции сил и средств, начиная со стандартизации, результатом которой является более высокий уровень оперативной и *информационной* совместимости [2].

Защита компьютерных систем от *киберугроз* при одновременной демонстрации соответствия требованиям законов и стандартов рассматривается как чрезвычайно сложная задача из-за трудностей с выбором приемлемого стандарта для использования. Более того, недостаток знаний о необходимых элементах, предлагаемых стандартом, а порой и отсутствие самого стандарта, приводит к проблеме определения *исходной* «точки» — ситуации, с которой можно начать организацию защиты.

Кроме того, многим организациям и компаниям не хватает опытного персонала в области кибербезопасности, поэтому им трудно внедрить стандартный подход или структуру обеспечения кибербезопасности [30]. Недостаточная осведомленность общественности о применении средств обеспечения кибербезопасности для защиты ИКТ-активов и информации (цифровых данных), принадлежащих частным лицам или организациям, может стать причиной фактической потери привилегированной информации.

Результаты анализа возможностей стандартизации в области кибербезопасности в сравнении с функционалом, реализованном в рамках отдельных пакетов или программ и антивирусных приложений, которые можно обобщить понятием *«рамочные структуры»* («РС»), приведены в табл. 3 [30].

Стандарты кибербезопасности — это наборы технических правил или практик, обычно используемых для

[14] Общероссийские классификаторы. URL: http://classifikators.ru/ (дата обращения: 29.02.24).

[15] ГОСТ Р 55062-2012. ИТ. Системы промышленной автоматизации и их интеграция. Интероперабельность. Основные положения. М. : Ростехрегулирование, 2013.

[16] Szenes Z. NATO Security Challenges and Standardization // Hadmérnök, XI. évf. 2016. T. 3. C. 285—298. URL: http://hadmernok.hu/163_23_ sze-nes.pdf (дата обращения: 29.02.24).

Таблица 3

Результаты сравнения подходов

Стандарты	«Рамочные структуры»
1. Добровольные документы, определяющие спецификации, процедуры и руководящие принципы для обеспечения безопасности, согласованности и надежности продуктов, услуг и систем. 2. Правила или документы, составленные на основе общего соглашения и одобренные юридическим лицом, которые определяют общее использование, регулирование, регламентацию или качество деятельности (масштаб предприятия). 3. Могут быть разработаны компанией (стандарт организации) или государством (ГОСТ). 4. Должны соблюдаться организацией-исполнителем в соответствии с нормативно-правовыми положениями. 5. Могут использоваться вместе с другими стандартами для дополнения и усиления отдельных требований. 6. Определяют, что должно быть сделано для соответствия стандарту. 6. Виды стандартов: - «открытые» — для всех типов предприятий и государственных организаций; - «закрытые» — для определенных (специфичных) отраслей или предприятий.	1. Общие руководства, которые могут быть приняты предприятиями (фирмами, учреждениями и др.), охватывающие многие компоненты или предметные области, но не определяющие шаги, которые необходимо предпринять. 2. Предоставляют только общее описание в качестве основы для создания чего-либо или достижения общей цели. 3. Используются для подведения итогов достижения целей, описания сферы охвата, руководства внедрением и оценкой, а также определения стандартов качества, которые должны быть достигнуты.

Рис 2. Согласование целей и задач обеспечения киберустойчивости на теоретическом и инженерно-техническом уровнях

защиты киберпространства или пользователей в организациях, имеющих подключение к ГТС. Целью внедрения стандартов кибербезопасности является повышение информационной безопасности, в первую очередь — инфраструктуры ИКТ, сетевых компьютерных систем, программного обеспечения и др. КВО. Стандарт также может определять функциональные требования и гарантии в процессах, системах, производственных средах, активах и технологиях.

Цели и задачи обеспечения киберустойчивости

Киберустойчивость представляет собой важное комплексное свойство сложных компьютерных систем, имеющее статистический характер и характеризующее их структуру (техническую, функциональную, программно-математическую)[17], рассматриваемое в качестве целевого фактора, ориентированного на кибербезопасность в приложениях программ «РС».

На рис. 2 показаны цели обеспечения киберустойчивости (вверху) и связанные с ними задачи (внизу) из «РС» (отдельных приложений) в области киберустойчивости [26].

[17] Бурый А.С. Введение в теорию синтеза отказоустойчивых многозвенных систем переработки навигационно-баллистической информации. М. : ВА им. Петра Великого, 1999. 299 с.

Планирование/подготовка. На данном этапе киберустойчивость обеспечивают, используя хорошо известные компоненты архитектуры, отношения и структуры с избыточностью, сегментацией, мониторингом, координацией и др. Осуществляется динамическая реконфигурация и перераспределение ресурсов КВО, используя динамическое представление и механизмы контроля целостности данных. *Понимание* (осознание), *подготовка* и *предупреждение* (***прогноз***) обеспечивают устойчивость на уровне применяемых программных платформ и ИКТ для взаимосвязи между операциями (оперативными процедурами) и этапами.

Усвоение. Продолжение операций или обеспечение выполнения миссии может потребовать непредвиденных изменений базовой архитектуры компьютерной системы в зависимости от того, что вышло из строя в результате кибератаки. Однако изменений могут потребовать не только компьютерные системы, но также *операционные процедуры* и *способ обмена информацией*. Следствием этого может быть необходимость альтернативной коммуникации и обработки данных наряду с изменением операционных процедур, что приводит к различным корпоративным архитектурам по горизонтали и вертикали, которые заранее не планировались, а реализуются по факту.

Восстановление. Конечное состояние этапа восстановления обычно поддерживается архитектурой. Однако переход из любого незапланированного состояния в восстановленное при сохранении непрерывности работы требует достаточно полного анализа вариантов переключений на этапе планирования, например, в ходе *имитационного моделирования* [11, 12]. Обеспечение свойств *гибкости* и *интероперабельности* позволит перепрофилировать кибер-ресурсы для резервирования мощностей и безопасного перехода на другой ресурс.

Адаптация. Этап перепроектирования часто является наиболее понятной частью процесса создания архитектуры киберустойчивости, поскольку физически понятно, как можно обеспечить реструктуризацию или реконфигурацию на основе предыдущих этапов, технических требований, а также возможностей применений новых технологий для повышения устойчивости с учетом модульности и гибкости управления кибер-ресурсами, перемещая и обновляя их.

Проблема стратегической устойчивости в области коллективной кибербезопасности

Стратегически важна постоянная *киберустойчивость* — устойчивость в области кибербезопасности. В виртуальном мире благодаря устойчивости в области кибербезопасности могут иметь место инновации, развитие, предпринимательство, демократия и пр.

В качестве основных частных свойств («составляющих») киберустойчивости функционирования компьютерной сети (информационного узла) в условиях существенной неопределённости и воздействия деструктивных кибератак можно рассматривать [12]:

- *информационную надежность* (технологическая составляющая), характеризующую степень защищённости обмена привилегированной информацией (выполнения функций криптопреобразования, маршрутизации и доставки информационных массивов, циркулирующих в сети) и заключающуюся в способности не допускать целенаправленного или случайного искажения, разрушения, раскрытия, модификации или переадресации информационных массивов;
- *информационную добротность* (целевая составляющая), характеризующую степень информационной экономичности функционирования компьютерной сети (узла) и заключающуюся в способности не допускать нецелевого расходования основных («работающих») видов системных ресурсов (информационно-содержательного и информационно-структурного) сети (узла).

Информационную надежность количественно можно определить как дополнение до 1 отношения средней («полной») условной энтропии $H(M_1|M_0)$ множества M_1 циркулирующих в сети криптограмм, соответствующего множеству M_0 исходных информационных массивов (массивов данных или программ), и безусловной энтропии множества M_1 [9, 28]:

$$J_N = 1 - H(M_1|M_0)/H(M_1) = 1 - \sum_i p(m_{0i})H(M_1|m_{0i})/H(M_1), \quad (1)$$

где $p(m_{0i} \in M_0)$, $i = 1,2,...$ — вероятность i-го исходного информационного массива из множества M_0 возможных; $H(M_1|m_{0i}) = \sum_j p(m_{1j}|m_{0i})\ln\{p(m_{1j}|m_{0i})\}$ — частная условная энтропия множества M_1 при фиксированном значении исходного информационного массива $m_{0i} \in M_0$; $H(M_1) = \sum_j p(m_{1j})\ln\{p(m_{1j})\}$ — безусловная энтропия множества M_1 криптограмм $m_{1j} \in M_1$, $j = 1,2,...$

При этом $J_N \in (0, 1]$ — информационная надежность равна 1 в случае отсутствия кибератак.

Информационную добротность можно определить как отношение общего количества I информации различного вида [12], хранящейся и циркулирующей в сети, и количества информации, характеризующего затраты основных видов системных ресурсов [13, 29]:

$$J_D = I/[I_v(\Theta)+I_z(T)], \quad (2)$$

где I — общее количество информации Q, которое хранится и циркулирует в сети (узле); $I_v(\Theta)$ — количество используемой *структурной* [12, 15] информации Q_v, содержащейся в сети (узле), имеющей структуру Θ, определяющее затраты (информационные, вещественные, энергетические) на преобразование содержательной осведомляющей информации Q_{zo}; $I_z(T)$ — количество *содержательной* информации Q_z в сети (узле), заключенной в ее общесистемном тезаурусе T (информационной базе).

Показатель (2) информационной добротности компьютерной сети (узла) позволяет, в частности, оценить экономичность действий сети (узла) в ходе информационного противоборства с субъектами кибератак на основе дополнительного учета в (2) в составе общего количества *I* информации *Q* следующих видов качественного проявления информации:

$Q_{zd1}(M,T)$; $Q_{zdj}(M,T)$, $j = 2,\ldots,J$ — «содержательной» дезинформации рассматриваемого и $J - 1$ враждебных субъектов, соответственно;

$Q_{s1}(N)$; $Q_{sk}(N)$, $k = 2,\ldots,K$ — структурно-статистической («шенноновской») информации о применении активных способов (методов) противоборства из определенного множества *N* возможных, заключенной в статистических структурах соответствующего множества сообщений о применении различных способов, при этом:

$$I_u(N) = -\sum_i p_i \ln(p_i),\ i = 1,\ldots,N,$$

где p_i — вероятность применения *i*-го способа (соответствующего сообщения-ИМ $m_i \in M$).

Концепция устойчивости признает стремление к обеспечению *готовности* для противодействия возможной интегративной составляющей возникающих кризисных явлений. Она рассматривается как инновационная процедура и инструмент политики стратегического управления. Именно на стратегическом уровне важен переход от «РС»-подхода к стандартизации процессов взаимодействия. В оборонном секторе, когда силы развертываются, им нужны гибкие и эффективные средства противодействия угрозам. Работая в сфере обеспечения кибербезопасности, они нуждаются в гибкости в оперативных действиях, ориентированных на сетевые технологии, мониторинг и *достоверные* (*помехоустойчивые, помехозащищённые* [11]) информационные потоки.

Стратегическая устойчивость в области коллективной кибербезопасности (*стратегическая киберустойчивость*) требует гибкой адаптации на уровне технологий и аппаратно-программных средств, постоянно расширяя инструменты сближения, интеграции и инноваций.

Последнее реализуется в концепции *«интеллектуальной обороны»* («смарт-обороны») *крупномасштабных* компьютерных систем (ККС), которая представляет собой измененный взгляд, лучшую стандартизацию и возможность для обновлений информационного взаимодействия на всех уровнях — от технологического до организационного, реализуя новые критически важные возможности. В частности, концепция *«умная оборона»* рассматривается в контексте *сотрудничества* НАТО с Европейским союзом по объединению и совместному использованию базисных ресурсов[18].

Прагматическое развитие данной концепции для определенной коалиции дружественных стран возможно на объединении и *совместном* использовании базисных и дополнительных ресурсов совокупности $A=\{a_1, a_2,\ldots a_m\}$ ККС a_i, $i = 1,\ldots,m$, каждая из которых характеризуется двумя агрегированными показателями, включая [15]:

$r_i \in R = \langle X, Y, Z, H \rangle$, $i = 1,\ldots,m$ — кортеж ресурсов, затрачиваемых на функционирование и развитие *i*-й ККС на протяжении её «жизненного цикла», где $X = \{x_1, x_2, \ldots x_m\}$, $Y = \{y_1, y_2, \ldots y_m\}$, $Z = \{z_1, z_2, \ldots z_m\}$ – множество значений величины кадровых (людские, оргштатные, интеллектуальные, административные), технико-экономических (средства, технологии, материалы, информация) и инфраструктурных (сетевые информационно-распределительные, транспортно-распределительные, энергетическо-распределительные) *базисных* ресурсов, соответственно; $H = \{h_1, h_2, \ldots h_m\}$ – множество значений параметров *дополнительных* «организационно-правовых» ресурсов;

$e_i = \sum_{ijk} \Delta t_{ijk} \big/ T_{\Pi}$, $i = \overline{1,m}$, $j = \overline{1,I}$, $k = x, y, z$ — уровень функциональной устойчивости *i*-й ККС, где Δt_{ijk} — временны*е* интервалы, на которых величины $r_{ijk} \in R$ ресурсов принимают значения ниже допустимого уровня; T_{Π} — временной интервал прогнозирования функционирования и развития совокупности ККС.

Любой проект распределения ресурсов допускает полное или частичное (в произвольной доле $\alpha_i \in [0,1]$) распределение ресурсов между различными ККС, причём при долевом распределении ресурсов показатели проекта сохраняются как $\alpha_i r_i$ и $\alpha_i e_i$ соответственно. В этом случае решение формализуется в виде обобщённого вектора $\alpha \in U$, $\alpha = \{\alpha_i \mid i = \overline{1,m}\}$ $\sum_{i=1}^{m} \alpha_i = 1$, который характеризует общие затраты ресурсов $R(\alpha, W) = \sum_{i=1}^{m} r_i(\alpha_i, W)$ и глобальную целевую функцию (ГЦФ) $E(\alpha) = \sum_{i=1}^{m} \alpha_i e_i$ уровня устойчивости функционирования совокупности ККС.

Максимизировать стратегическую киберустойчивость — устойчивость (стабильность) функционирования совокупности ККС (т. е. минимизировать значение ГЦФ) и при этом не допустить снижения эффективности Ф применения (функционирования) каждой ККС и превышения расходования заданного общего количества R^0 ресурсов возможно, решив проблему в виде:

$$\begin{cases} E(\alpha, w^*) = \min\limits_{w_j \in W} \\ R(\alpha, w^*) \le R^0;\ \Phi_i \in \Delta\Phi_i^0, \end{cases} \qquad (3)$$

где $W = \{w_j(\psi)\}$, $j = \overline{1,n}$ — множество допустимых стратегий обеспечения ресурсами; ψ — координирующий параметр применения ресурсов; a_i, $i = 1,\ldots,m$ — весовой коэффициент; $E = \langle e_1, e_2, \ldots, e_m \rangle$ — вектор уровней функциональной устойчивости (локальных целевых функций — ЛЦФ) совокупности

[18] В настоящее время сотрудничество НАТО с рядом государств, включая Россию, Иран, Северную Корею и Китай, приостановлено согласно Стратегии национальной кибербезопасности США 2018 г.

ККС; $\Delta\Phi_i^0$ — допустимый диапазон значений эффективности применения *i*-й ККС.

Решение проблемы (3) возможно в ходе многоагентного имитационно-игрового поиска оптимальной согласованной стратегии-решения $w^* \in W$ обеспечения (предоставления и координации применения) базисными и дополнительными ресурсами, при использовании которой функционирование и развитие *совокупности* крупномасштабных ККС в условиях деструктивного воздействия кибератак будет *устойчивым* (стабильным) на интервале прогнозирования при условии обеспечения эффективности целевого применения ККС с учётом ограничения на общее количество распределяемых ресурсов [1, 15].

Заключение

Внедрение высоких технологий связано с появлением новых технологических рисков, появление которых необходимо прогнозировать, к ним следует готовиться заранее и разрабатывать соответствующие методы управления, чтобы минимизировать степень деструктивного воздействия кибератаки или, по возможности, купировать. Сложность управления рисками обусловлена тем, что риски внедрения новых технологий очень разнообразны: появление новых вирусных программ, угрозы внешнего управления, исчезновения приватности, тайная слежка, утечка персональных данных, контроль рынка и др.

Ввиду того, что при рассмотрении вопросов обеспечения кибербезопасности следует учитывать ее влияние на безопасность политическую, технологическую и социальную, то ряд приложений и конкретные направления организационной деятельности следует рассматривать через призму их решения военными зарубежными альянсами. Не случайна же военная направленность применяемых терминов в этой сфере: *кибератака, кибершпионаж, кибертерроризм, кибервойна*. Операции кибервойн могут включать действия шпионажа, взлома, дестабилизации компьютерных систем, распространения нежелательного программного обеспечения и др. Кибервойны часто также направлены на создание хаоса и паники среди населения эвентуального противника или нарушение жизнедеятельности страны.

Киберзащита может использоваться в качестве основной политики интеллектуальной обороны («умной обороны»), регулируя скоординированный уровень тактического военного и гражданского потенциала и развертывания потенциала в тактических симметричных или асимметричных операциях.

При всей важности вопросов кибербезопасности следует заметить, что в реальной жизни существует множество факторов, из-за которых компьютерные системы могут выйти из строя не только по причинам воздействия хакерской целенаправленной атаки, внедрения вредоносного программного обеспечения или мошенничества. Иногда это просто проявление халатности, допущения ошибок, недостатка компетенции или недобросовестных действий (бездействия) со стороны персонала [4, 11]. Поэтому к критериям защищенности нужно отнести не только защиту от внешних или случайных атак, но и инструменты предупреждения и предотвращения некорректных или ошибочных действий со стороны собственных сотрудников. Вот почему актуальным становится социальный запрос о необходимости ведения образовательной деятельности [20] среди населения по совершенствованию культуры информационной безопасности (включая кибербезопасность).

В статье подчеркивается важность обеспечения кибербезопасности как стратегического направления поддержки ИКТ, одновременно отражая необходимость в постоянно совершенствуемых методах обеспечения безопасности в целях разработки единого методологического подхода к информационной защите нынешней и будущей информационной инфраструктуры современного общества.

Обоснованы количественные показатели целевой (информационная добротность) и технологической (информационная надежность) составляющих устойчивости как целевого фактора, ориентированного на кибербезопасность. Формализована проблема стратегической устойчивости в области коллективной кибербезопасности и предложен путь ее решения на основе многоагентного имитационно-игрового моделирования, для которого разработан базовый программный комплекс.

Рецензент: ***Цимбал Владимир Анатольевич,*** *доктор технических наук, профессор, заслуженный деятель науки РФ, профессор кафедры автоматизированных систем боевого управления Филиала Военной академии им. Петра Великого, г. Серпухов, Российская Федерация.*
E-mail: tsimbalva@mail.ru

Литература

1. Базовый программный комплекс имитационно-игрового моделирования «БПК MEIS-DM». Свидетельство № 2013615257 РФ / Д.А. Ловцов, Н.А. Сергеев, В.Н. Гаврилов, А.Б. Ермолаева (РФ). № 2013613471/09; заяв. 26.04.13; зарег. 03.06.13 // Бюл. 2013. № 6.
2. Бурый А.С. Состояние и тенденции развития стандартизации государств — членов НАТО // Стандартизация военной техники. 2023. № 2. С. 46—53.
3. Валиахметова Г. Н., Цуканов Л.В. «Сумма всех ресурсов страны»: специфика израильского подхода *к обеспече*нию национальной кибербезопасности // Уральское востоковедение. 2021. № 11. С. 23—34.
4. Духвалов А.П. Кибератаки на критически важные объекты — вероятная причина катастроф // Вопросы кибербезопасности. 2014. № 3 (4). С. 50—53.
5. Карцхия А.А. Правовые аспекты современной киберпреступности // Правовая информатика. 2023. № 1. С. 40—48. DOI: 10.21681/1994-1404-2023-1-40-48 .
6. Круглов В.В., Ловцов Д.А. Концепция информационно-ударной операции в современной войне // Обозреватель-Observer. 1999. № 12. С. 49—51.
7. Курылев К.П., Цаканян В.Т. Цифровая зависимость НАТО // Вестник Московского государственного областного университета. Сер.: История и политические науки. 2018. № 1. С. 45—53.
8. Лебедь С.В. Инновационные технологии в сфере кибербезопасности // Современные информационные технологии и ИТ-образование. 2022. Т. 18. № 2. С. 383—390.
9. Ловцов Д.А. Информационная надёжность функционирования телематической сети ГАС РФ «Правосудие» // Правовая информатика. 2018. № 1. С. 40—48. DOI: 10.21681/1994-1404-2018-1-40-48
10. Ловцов Д.А. О концепции комплексного подхода // Философские исследования. 2000. № 4. С. 158—174.
11. Ловцов Д.А. Теория защищенности информации в эргасистемах : монография. М. : РГУП, 2021. 276 с. ISBN 978-5-93916-896-0.
12. Ловцов Д.А. Информационная теория эргасистем : монография. М. : РГУП, 2021. 314 с. ISBN 978-5-93916-887-8.
13. Ловцов Д.А. Эффективность правовых эргасистем в инфосфере // Правовая информатика. 2020. № 1. С. 4—14. DOI: 10.21681/1994-1404-2020-1-04-14 .
14. Ловцов Д.А., Ермаков И.В. Классификация и модели нетрадиционных информационных каналов в эргасистеме // НТИ РАН. Сер. 2. Информ. процессы и системы. 2005. № 2. С. 1—7.
15. Ловцов Д.А., Сергеев Н.А. Управление безопасностью эргасистем : монография / Под ред. Д. А. Ловцова. 2-е изд., испр. и доп. М. : РАУ—Университет, 2001. 224 с.
16. Ловцов Д.А., Федичев А.В. Архитектура национального классификатора правовых режимов информации ограниченного доступа // Правовая информатика. 2017. № 2. С. 35—54. DOI: 10.21681/1994-1404-2017-2-35-54 .
17. Малаев А.Х. Применение цифровых технологий и искусственного интеллекта при предупреждении экстремистских и террористических преступлений // Пробелы в российском законодательстве. 2023. Т. 16. № 4. С. 263—267.
18. Малюк А.А., Полянская О.Ю. Зарубежный опыт формирования в обществе культуры информационной безопасности // Безопасность информационных технологий. 2016. Т. 23. № 4. С. 25—37.
19. Манойло А.В. Современные стратегии кибербезопасности и кибероборонны НАТО // Актуальные проблемы Европы. 2020. № 3 (107). С. 160—184.
20. Махалин В.Н., Махалина О.М. Управление вызовами и угрозами в цифровой экономике России // Управление. 2018. Т. 6. № 2. С. 57—60.
21. Плеханова О.А. Безопасность киберфизических систем на предприятиях // Экономический вестник. 2023. Т. 2. № 2. С. 17—21.
22. Скиба В.А., Скиба Н.П. Кибернетическая среда функционирования корпоративных систем // Правовая информатика. 2022. № 4. С. 40—48. DOI: 10.21681/1994-1404-2022-4-40-48 .
23. Терентьева Л.В. Управление киберпространством в условиях противостояния России и стран североатлантического альянса // Правовая информатика. 2022. № 3. С. 40—48. DOI: 10.21681/1994-1404-2022-3-40-48 .
24. Burton J. NATO's cyber defence: strategic challenges and institutional adaptation // Defence Studies. 2015. Vol. 15. No. 4. Pp. 297–319.
25. Jasper S. Strategic cyber deterrence: The active cyber defense option. Rowman & Littlefield, 2017.
26. Kott A. et al. Approaches to enhancing cyber resilience: Report of the North Atlantic Treaty Organization (NATO) workshop IST-153 // arXiv preprint, arXiv: 1804.07651.2018.
27. Kutlu F.B. A New Field Between Two Old Allies: Cybersecurity Approaches of EU and NATO (2016—2020) // Journal of Diplomatic Research. 2023. Vol. 5. No. 1. Pp. 24–41.
28. Lovtsov D.A. Informational Indexes of Efficiency of Control Systems for Complex Dinamic Objects // Automation and Remote Control. 1994. Vol. 55. No. 12. Part 2. Pp. 1824–1829.
29. Lovtsov D.A. Models for Measuring the Information Resource of a Computerized Control System // Automation and Remote Control. 1996. Vol. 57. No. 9. Part 1. Pp. 1221–1232.

30. Syafrizal M., Selamat S. R., Zakaria N. A. Analysis of cybersecurity standard and framework components // International Journal of Communication Networks and Information Security. 2020. Vol. 12. No. 3. Pp. 417–432.

CYBERSECURITY: THE MAIN TENDENCIES IN ENSURING

Dmitrii Lovtsov, *Dr.Sc. (Technology), Professor, Honoured Scientist of the Russian Federation, Deputy Director for Research of the Lebedev Institute of Precision Mechanics and Computer Engineering of the Russian Academy of Sciences, Head of the Department of Information Technology Law, Informatics and Mathematics of the Russian State University of Justice, Moscow, Russian Federation.*
E-mail: dal-1206@mail.ru

Aleksei Buryi, *Dr.Sc. (Technology), Department Director at the Russian Standardisation Institute, Leading Researcher at the Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Moscow, Russian Federation.*
E-mail: a.s.burij@gostinfo.ru

Keywords: *cybersecurity, computer systems, critical information infrastructure, critically important facilities, information and communication technologies, information space, cyberattacks, cybersphere, standardisation, cybersustainability, information reliability, information quality factor, problem.*

Abstract

Purpose of the work: improving the research and methodological basis of the theory of information protection and security in critically important facilities.

Methods used in the study: system and expert analysis, logical concept modelling, formal logical development and justification of the mathematical structure of the strategic cybersustainability problem.

Study findings: a general description of cybersecurity as a property of computer systems is given. The basic concepts and definitions, tendencies and approaches in ensuring cybersecurity in Russia and NATO are considered. The possibilities for standardisation of the cybersphere as well as the goals and tasks of ensuring cybersustainability as a target factor oriented at cybersecurity are identified. Justifications are given for specific numerical indicators and criteria of cybersustainability. As regards the strategic sustainability problem in the field of collective cybersecurity, a justification is given for its mathematical structure and a way for solving the problem is put forward. General recommendations are given for ensuring cyberprotection in strategic network operations.

References

1. Bazovyi programmnyi kompleks imitatsionno-igrovogo modelirovaniia "BPK MEIS-DM". Svidetel'stvo No. 2013615257 RF. D.A. Lovtsov, N.A. Sergeev, V.N. Gavrilov, A.B. Ermolaeva (RF). No. 2013613471/09; zaiav. 26.04.13; zareg. 03.06.13. Biul., 2013, No. 6.
2. Buryi A.S. Sostoianie i tendentsii razvitiia standartizatsii gosudarstv – chlenov NATO. Standartizaciya voennoj tekhniki, 2023, No. 2, pp. 46–53.
3. Valiakhmetova G. N., Tsukanov L.V. "Summa vsekh resursov strany": spetsifika izrail'skogo podkhoda k obespecheniiu natsional'noi kiberbezopasnosti. Ural'skoe vostokovedenie, 2021, No. 11, pp. 23–34.
4. Dukhvalov A.P. Kiberataki na kriticheski vazhnye ob"ekty – veroiatnaia prichina katastrof. Voprosy kiberbezopasnosti, 2014, No. 3 (4), pp. 50–53.
5. Kartskhiia A.A. Pravovye aspekty sovremennoi kiberprestupnosti. Pravovaia informatika, 2023, No. 1, pp. 40–48. DOI: 10.21681/1994-1404-2023-1-40-48 .
6. Kruglov V.V., Lovtsov D.A. Kontseptsiia informatsionno-udarnoi operatsii v sovremennoi voine. Obozrevatel'-Observer, 1999, No. 12, pp. 49–51.
7. Kurylev K.P., Tsakanian V.T. Tsifrovaia zavisimost' NATO. Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Ser.: Istoriia i politicheskie nauki, 2018, No. 1, pp. 45–53.
8. Lebed' S.V. Innovatsionnye tekhnologii v sfere kiberbezopasnosti. Sovremennye informatsionnye tekhnologii i IT-obrazovanie, 2022, t. 18, No. 2, pp. 383–390.

9. Lovtsov D.A. Informatsionnaia nadezhnost' funktsionirovaniia telematicheskoi seti GAS RF "Pravosudie". Pravovaia informatika, 2018, No. 1, pp. 40–48. DOI: 10.21681/1994-1404-2018-1-40-48
10. Lovtsov D.A. O kontseptsii kompleksnogo podkhoda. Filosofskie issledovaniia, 2000, No. 4, pp. 158–174.
11. Lovtsov D.A. Teoriia zashchishchennosti informatsii v ergasistemakh : monografiia. M. : RGUP, 2021. 276 pp. ISBN 978-5-93916-896-0.
12. Lovtsov D.A. Informatsionnaia teoriia ergasistem : monografiia. M. : RGUP, 2021. 314 pp. ISBN 978-5-93916-887-8.
13. Lovtsov D.A. Effektivnost' pravovykh ergasistem v infosfere. Pravovaia informatika, 2020, No. 1, pp. 4–14. DOI: 10.21681/1994-1404-2020-1-04-14 .
14. Lovtsov D.A., Ermakov I.V. Klassifikatsiia i modeli netraditsionnykh informatsionnykh kanalov v ergasisteme. NTI RAN. Ser. 2. Inform. protsessy i sistemy, 2005, No. 2, pp. 1–7.
15. Lovtsov D.A., Sergeev N.A. Upravlenie bezopasnost'iu ergasistem : monografiia. Pod red. D. A. Lovtsova. 2-e izd., ispr. i dop. M. : RAU–Universitet, 2001. 224 c.
16. Lovtsov D.A., Fedichev A.V. Arkhitektura natsional'nogo klassifikatora pravovykh rezhimov informatsii ogranichennogo dostupa. Pravovaia informatika, 2017, No. 2, pp. 35–54. DOI: 10.21681/1994-1404-2017-2-35-54 .
17. Malaev A.Kh. Primenenie tsifrovykh tekhnologii i iskusstvennogo intellekta pri preduprezhdenii ekstremistskikh i terroristicheskikh prestuplenii. Probely v rossiiskom zakonodatel'stve, 2023, t. 16, No. 4, pp. 263–267.
18. Maliuk A.A., Polianskaia O.Iu. Zarubezhnyi opyt formirovaniia v obshchestve kul'tury informatsionnoi bezopasnosti. Bezopasnost' informatsionnykh tekhnologii, 2016, t. 23, No. 4, pp. 25–37.
19. Manoilo A.V. Sovremennye strategii kiberbezopasnosti i kiberoborony NATO. Aktual'nye problemy Evropy, 2020, No. 3 (107), pp. 160–184.
20. Makhalin V.N., Makhalina O.M. Upravlenie vyzovami i ugrozami v tsifrovoi ekonomike Rossii. Upravlenie, 2018, t. 6, No. 2, pp. 57–60.
21. Plekhanova O.A. Bezopasnost' kiberfizicheskikh sistem na predpriiatiiakh. Ekonomicheskii vestnik, 2023, t. 2, No. 2, pp. 17–21.
22. Skiba V.A., Skiba N.P. Kiberneticheskaia sreda funktsionirovaniia korporativnykh sistem. Pravovaia informatika, 2022, No. 4, pp. 40–48. DOI: 10.21681/1994-1404-2022-4-40-48 .
23. Terent'eva L.V. Upravlenie kiberprostranstvom v usloviiakh protivostoianiia Rossii i stran severoatlanticheskogo al'iansa. Pravovaia informatika, 2022, No. 3, pp. 40–48. DOI: 10.21681/1994-1404-2022-3-40-48 .
24. Burton J. NATO's cyber defence: strategic challenges and institutional adaptation. Defence Studies. 2015. Vol. 15. No. 4. Pp. 297–319.
25. Jasper S. Strategic cyber deterrence: The active cyber defense option. Rowman & Littlefield, 2017.
26. Kott A. et al. Approaches to enhancing cyber resilience: Report of the North Atlantic Treaty Organization (NATO) workshop IST-153. arXiv preprint, arXiv: 1804.07651.2018.
27. Kutlu F.B. A New Field Between Two Old Allies: Cybersecurity Approaches of EU and NATO (2016–2020). Journal of Diplomatic Research. 2023. Vol. 5. No. 1. Pp. 24–41.
28. Lovtsov D.A. Informational Indexes of Efficiency of Control Systems for Complex Dinamic Objects. Automation and Remote Control. 1994. Vol. 55. No. 12. Part 2. Pp. 1824–1829.
29. Lovtsov D.A. Models for Measuring the Information Resource of a Computerized Control System. Automation and Remote Control. 1996. Vol. 57. No. 9. Part 1. Pp. 1221–1232.
30. Syafrizal M., Selamat S. R., Zakaria N. A. Analysis of cybersecurity standard and framework components. International Journal of Communication Networks and Information Security. 2020. Vol. 12. No. 3. Pp. 417–432.