При использовании материалов статьи необходимо использовать данную ссылку:
Бурый А.С., Усцелемов В.Н. Онтологический подход к формированию когнитивных моделей оценки кибербезопасности // Информационно-экономические аспекты стандартизации и технического регулирования. 2020. № 3. (55). С. 77-84

УДК 004.056

ОНТОЛОГИЧЕСКИЙ ПОДХОД К ФОРМИРОВАНИЮ КОГНИТИВНЫХ МОДЕЛЕЙ ОЦЕНКИ КИБЕРБЕЗОПАСНОСТИ

Бурый А.С., Усцелемов В.Н.

Рассматриваются вопросы обеспечения кибербезопасности функционирования информационных систем в условиях больших данных, вызванных ростом количества информационных источников.
Для повышения кибербезопасности современных информационных систем предлагается методический подход, включающий: 1) анализ киберпространства, на основе разработки онтологических структур понятийных событий (сценарных цепочек типовых действий) для выявления киберугроз и возможных опасностей; 2) разработку когнитивных моделей оценки кибербезопасности информационных систем для организации парирования кибератак с привлечением аналитики больших данных.
Кибер-онтологии предлагается рассматривать, как адаптивные словари данных, приложений и взаимосвязей с пользователями для улучшения сценариев поведения и анализа с целью исключения распространения угроз до начала их возникновения. Рассмотренная онтологическая структура позволяет систематизировать возможные источники угроз и принимать защитные меры, осуществлять мониторинг киберпространства с целью оценки уязвимостей, и уровня рисков в различных сочетаниях угроз и принимаемых мер по их устранению.

Ключевые слова: кибербезопасность, киберпространство, киберугрозы, структурирование знаний, онтологический инжиниринг, когнитивные модели.

Введение

В существующей реальности цифровой трансформации в мире приходится переосмысливать стратегии кибербезопасности в условиях участившихся фактов информационных провокаций, преднамеренных проникновений и взломов информационных систем с целью нанесения ущерба организациям или организационным структурам и отдельным лицам. Для мировой экономики киберугрозы по своим последствиям вышли на третье место вслед за проблемами, вызванными изменением климата и стихийными бедствиями. Международный уровень проблемы кибербезопасности закреплен и в рамках стандартов ISO/IEC (Международная Организация по Стандартизации / Международная Электротехническая Комиссия), где действует технический комитет и комиссия экспертов по разработке международных стандартов в области информационной безопасности (ИБ) [1]. Направлением серии стандартов ISO 27000 выступают «*Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности*» содержащее около 30 стандартов, бóльшая часть которых имеет статус ГОСТ Р, что подтверждает важность и востребованность данной серии. Концептуальный аспект данной серии стандартов помогает специалистам в области кибербезопасности с единой терминологической платформы проводить мероприятия по обеспечению безопасности аппаратно-программных средств и активов организаций [2].

Бурый Алексей Сергеевич, доктор технических наук, директор департамента, ФГУП «СТАНДАРТИНФОРМ»
г. Москва
Усцелемов Вячеслав Николаевич, соискатель,
ФГУП «СТАНДАРТИНФОРМ»,
г. Москва

Для информационных технологий (ИТ) и информационных систем (ИС) актуальным является оценка возможности нанесения ущерба организации за счет выявления нарушителями уязвимостей активов, что объединяется в понятии риска информационной безопасности. Исходя из сущности ИБ, риски связаны с составляющими ИБ – конфиденциальностью, целостностью и доступностью информации в ИС, поэтому существующая система управления риском ИБ направлена на снижение риска путем организационных, технологических, программных и других мер. Риск будем рассматривать как меру степени опасности, вероятность причинения вреда или вероятность негативных последствий активам организации [3].

При моделировании кибер-сценариев для повышения ситуационной осведомленности операторов по безопасности, а также обычных пользователей актуальным становится смещение акцента с системного уровня представления ИБ, как подсистемы автоматизированной информационной системы в целом [4] или отдельных ее сегментов [5] на уровень окружающей среды. Для обоснованности принятия решений разрабатываются модели управления, учитывающие: 1) временные и технологические ограничения, например, при решении динамических задач в эргасистемах [6,7] и в многоагентных моделях общесистемного проектирования [8]; 2) ограничения, вызванные неопределенностями в проявлении несанкционированного вмешательства в инфраструктуру ИС [9]; 3) методику принятия решений в условиях роста объема и ценности данных на основе игровых моделей [10] или в условиях случайной смены структур при многозвенной переработке измерительных данных [11].

Возможности машинного обучения и аналитика больших данных (Big Data) в первую очередь направлены на выявление новых знаний из данных, формируемых многочисленными датчиками, сервисными пакетами и программными модулями в разнообразной палитре практического применения [12,13]. Умение извлекать информацию из данных, объемы которых растут год от года, становится гарантией конкурентных преимуществ современных технологий, организаций и программно-аналитических комплексов. Практика показывает, что злоумышленники используют любые возможности несанкционированного доступа к данным, как единичных пользователей, так и базам данных отдельных организаций. По итогам 2019 г. 16% нарушений затронули государственный сектор, 15% нарушений – отрасль здравоохранения, затем следует финансовая сектор – 10% [14].

Целью представленного исследования является формирование методического подхода к обеспечению кибербезопасности современных информационных систем, на основе онтологического представления анализируемого киберпространства и выявления в нем новых понятийных событий при выявлении киберугроз и организации парирования кибератак с привлечением аналитики больших данных.

Онтологический аспект структурирования знаний

Исследование знаний в любой предметной области предполагает их структуризацию, формальное описание, анализ процесса их накопления, а также управление знаниями в ходе решения ИС целевых задач.

На концептуальном уровне для представления знаний в таком активно развивающемся научном направлении, как кибербезопасность, требуется постоянно анализировать существующее киберпространство в ходе взаимодействия человек – компьютер, посредством сетевых и телекоммуникационных технологий, в котором политика безопасности и конфиденциальности играют первостепенную роль.

Онтологический аспект любого исследования позволяет сформировать структурное представление описания определенной реальности (предметной области), за счет системы понятий, связанных с помощью логических отношений «общее – единичное». Словарь понятий строится на терминологии нормативно–методических документов и стандартов в области информационных технологий и кибербезопасности [1-3].

Применение онтологий обусловлено необходимостью структурирования, форматирования и унификации представления знаний, а также устранения терминологической несогласованности с целью их многократного и гибкого использования в информационных системах [15].

Структура онтологии определяется:

видом предметной области;

целями онтологического инжиниринга [16];

уровнем применяемых методов и алгоритмов идентификации и типами киберугроз [4,5], их взаимовлиянием друг на друга;

комплексом защиты и обнаружения возможных уязвимостей [17].

Онтологический инжиниринг рассматривается как инженерия знаний применительно к компьютерным системам для решения задач информационного обеспечения в подсистемах автоматизированных систем проектирования, принятия решений, информационного поиска на основе семантического описания пространства знаний [16].

Онтологические модели характеризуются статичностью, что сказывается на возможности обновления понятийного аппарата. Однако существующие модели помогают учитывать различные гетерогенные компоненты ИТ и элементы кибербезопасности рассматривать в совокупности.

Для исследования взаимосвязей и взаимовлияний между основными понятиями (элементами) киберпространства разрабатываются онтологические структуры [15-17] (см. рисунок 1) для прогнозирования возможных уязвимостей и сценариев парирования кибератак для уменьшения рисков потери активов при организации противодействия компьютерным атакам.

Стейкхолдеры (stakeholders) на рисунке 1 представляют собой как внутренние, так и внешние заинтересованные в защите своих активов стороны. Онтологические структуры, по сути, являются когнитивными схемами формирования знаний при решении задач кибербезопасности ИС для выбранной предметной области.

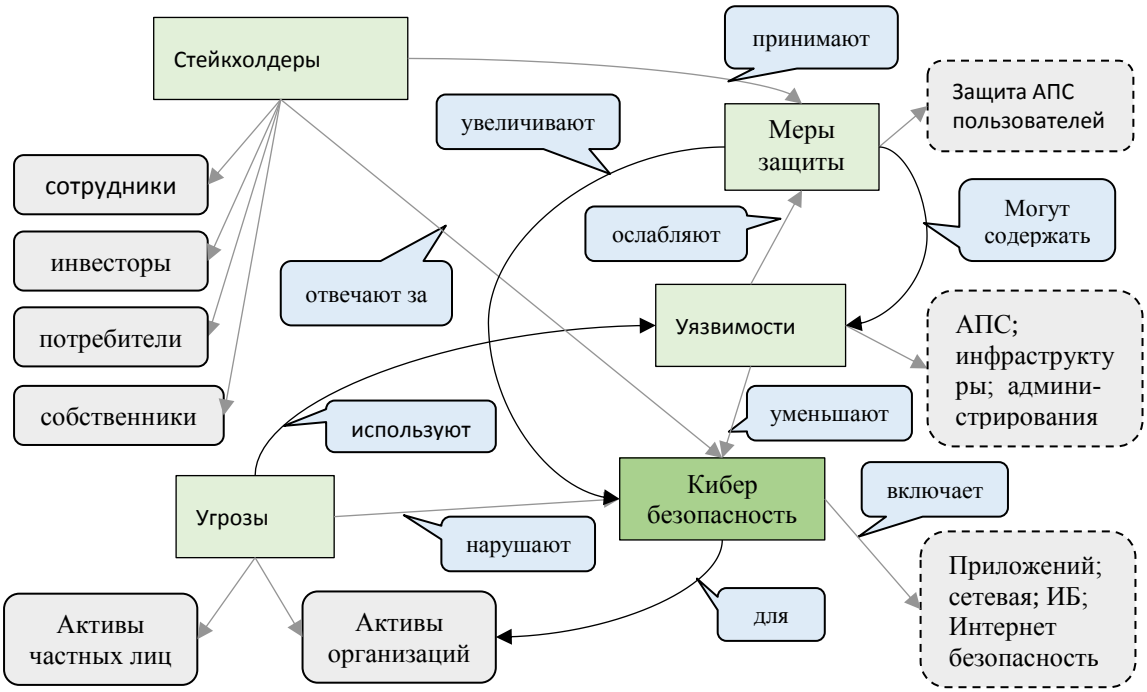

Рисунок 1. Группы факторов, составляющих онтологию кибербезопасности

Основной задачей онтологии является не только терминологическое описание выбранной предметной области (эксплицитная форма знаний), но и обеспечение их структуризации на основе системы отношений, т.е. структуризации взаимовлияний (уровень имплицитного представления знаний), построенной на интуиции, когнитивном мышлении, опыте исследований.

Когнитивные подходы к оценке информационной безопасности

Отличительной стороной кибер-рисков от рисков, например, в области надежности, эксплуатации техники и других, в том, что инциденты в области кибербезопасности являются высокоскоростными событиями разнообразной природы и проявлений. Злоумышленники или атакующая сторона (АтС) зачастую делают ставку на масштабность атаки, сложность ее динамики, некомпетентность большинства сотрудников, пытающихся самостоятельно противостоять атакам. Отталкиваясь от известной цитаты из Н.В. Гоголя, что «редкая птица долетит до середины Днепра», можно утверждать, что у особо «одаренных» АтС редкая атака не приводит к положительному результату.

С развитием аналитики больших данных в условиях совершенствования компьютерных методов анализа появляются новые возможности по выявлению попыток несанкционированного доступа злоумышленников в ИС.

Исторически, начиная с 60-х годов прошлого века, стали разрабатываться методы машинного обучения, основным содержанием которых являлись задачи классификации, предсказания (прогнозирования) и продукционного вывода, что активно использовалось при построении экспертных систем, а также в системах поддержки принятия решений автоматизированных комплексах различного назначения. В 80-е годы характеризуются активной разработкой методов интеллектуального анализа данных, получивших название Data Mining (DM), обеспечивающих обнаружение в данных ранее неизвестных новых признаков (свойств).

Дальнейшее развитие это направление получило в 90-е годы под названием Knowledge Discovery in Databases (KDD) или «Поиск и выявления знаний в данных». Помимо традиционных этапов предварительной обработки данных подготовки данных, формирования признаков и шаблонов, производится выявления полезных знаний на основе известных методов DM или их расширения:

Таким образом, KDD использует методы DM, чтобы получить новые знания, а последовательность его шагов не зависит от предметной области. Методы интеллектуального анализа данных настроены на решение следующих основных классов задач:

- построение ассоциативных правил;
- кластеризации;
- классификации;
- прогнозирования;
- регрессионного анализа.

В классификационных алгоритмах цена ошибок при выявлении вторжений и аномалий всегда велика, т.к. АтС стремится обойти систему выявления аномалий. Поэтому требуется оценить структурные возможности системы КБ, чтобы снизить риски, выявить уязвимости и продумать организационные и технологические меры защиты ИС, для чего воспользуемся методом когнитивного моделирования.

Когнитивное моделирование (КМ) – способ анализа совокупности взаимообусловленных факторов, обеспечивающих целевое управление исследуемым объектом. В результате когнитивного анализа формируются причинно-следственные графы, характеризующие взаимодействие факторов с учетом качественного и количественного выражения технологических, информационных и организационных факторов-воздействий. Основной особенностью когнитивного подхода является возможность учета слабоструктурированных процессов, влияющих на целевой фактор, за который в рассматриваемой задаче выбрана кибербезопасность.

Для случая представления концептов (факторов), влияющих на кибербезопасность ИС, в виде нечеткой когнитивной карты (НКК), граф – Γ которой можно представить в виде [18, 19]:

$$\Gamma = \langle B, R, W \rangle, \quad (1)$$

где $B = \{1, 2, ..., n\}$ – множество вершин графа (концептов, факторов), описывающих ситуацию моделирования; $R \subseteq B \times B$ – множество дуг (причинно-следственных связей между концептами), причем $R = \{r_{ij} \mid r_{ij} \in R;\ i, j = \overline{1,n}\}$, где n – число вершин Γ, а r_{ij} – есть влияние фактора i на фактор j; W – множество весов (характеристик) связей. Влияние концептов в графе представим в виде [18] нечетких бинарных отношений $r_{ij} \in [0,1]$. При этом положительные связи («+») соответствую росту фактора- «следствия» относительно фактора - «причины», а для отрицательных весов связей («–») – эффект обратный [19].

Формирование модели НКК в большинстве случаев осуществляется экспертами и подчиняется логике взаимовлияния выделенных концептов. Для простоты воспользуемся факторами, выделенными на рис. 1, оставив наиболее существенные из них (см. рис. 2). Естественно будет предположить, что учет бóльшего количества факторов позволит повысить адекватность разрабатываемой когнитивной модели. Однако в методическом плане можно воспользоваться и упрощенным подходом, указав условия, для которых справедлив данный подход, а именно: при неограниченных ресурсах на организацию мер защиты. При обосновании весов связей из (1) экспертам могут быть поставлены дополнительные ограничения на выбор начальных значений нагрузок рассматриваемых связей.

Таким образом, КМ в задачах обеспечения кибербезопасности ИС пересекается с процедурами экспертного оценивания

выбираемых концептов модели и параметров связей. Например, связь концептов B_5 и B_6 равна +0,4 , тогда рост концепта B_5 на 20% обеспечит рост безопасности активов организации (концепт B_6) на 50%.

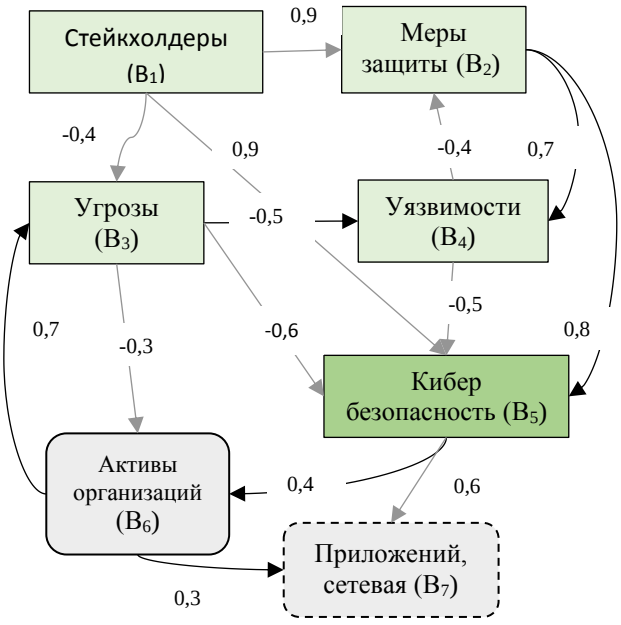

Рисунок 2. Структура НКК оценки факторов влияния

В рассматриваемой задаче целевым концептом является обеспечение кибербезопасности информационной системы – концепт B_5 , на который влияют, как непосредственно связанные с ним концепты (B_1 – B_4), так и сценарные цепочки, для которых B_5 выступает промежуточным звеном, например, для контура $B_3 \to B_4 \to B_5 \to B_6$.

Экспертные методы чаще формируют качественные оценки, получаемые на основе мнений специалистов определенной области знаний. Типовые задачи экспертных методов: определение вероятностей событий и временных интервалов на множестве событий; структурирование проблем и определение приоритетности решения проблем; дифференцирование целей управления до задач и определение приоритетности их решения; генерирование альтернатив; фильтрация множества альтернатив и оценка их предпочтения.

Рекомендации по безопасности при удаленной работе

При удаленной работе потенциал Интернета открывается, как в виде бóльших возможностей для пользователей, так и в виде дополнительных рисков в вопросах безопасности, к которым можно отнести незащищенность сети Wi-Fi; персональных устройств, домашних сетей, фактически обладающих более слабыми защитными свойствами, по сравнению с сетевыми и программными средствами защиты организаций.

К простейшим правилам при дистанционной работе, особенно, когда с одним документом работают несколько сотрудников, отнесем следующие:

- использование надежных паролей;
- использование лицензированного, в том числе и антивирусного, программного обеспечения;
- обязательная практика обновления программного обеспечения;
- создание резервных копий данных;
- особая осторожность при получении фишинговых почтовых рассылок;
- настройка брандмауэров, контролирующих, а иногда и запрещающих процесс скачивания файлов из непроверенных источников и обеспечивающих отражение преднамеренных воздействий;
- защита домашних маршрутизаторов.

Работодатели обязаны подготовить для персонала инструкции по действиям в случае возникновения проблем с ИБ и продумать меры для защиты корпоративной информации и организовать адекватную оперативную информационную поддержку для устранения возможных проблем.

Выводы

Современные структуры онтологий превращаются в активного поставщика связей элементов данных с использованием методов машинного обучения, интеллектуального анализа данных для адаптации к среде применения.

Кибер-онтологии можно рассматривать, как адаптивные словари данных, приложений и взаимосвязей с пользователями для улучшения сценариев поведения, анализа и помощи по исключению распространения угроз до начала их возникновения. Рассмотренная онтологическая структура позволяет систематизировать возможные источники угроз, мероприятия по противодействию им, выполнить мониторинг киберпространства с целью оценки уязвимостей, и уровня рисков в различных сочетаниях угроз и принимаемых мер по их устранению.

Оценку структурных возможностей организации системы кибербезопасности можно проводить на основе построения когнитивных моделей, весовые параметры связей в которых выбираются экспертными методами, а итоговый

вектор нагрузок для целевого концепта определяется путем когнитивного моделирования относительно НКК. iea

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ:

1. ГОСТ Р ИСО/МЭК 27000-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. – М.: Стандартинформ, 2019.
2. Марков А.С., Цирлов В.Л. Руководящие указания по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. 2014. № 1(2). С. 28-35.
3. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – М.: Стандартинформ, 2011. – 50 с.
4. Бурый А.С., Усцелемов В.Н. Организация информационной безопасности в автоматизированных системах управления // Информационно-экономические аспекты стандартизации и технического регулирования. 2016. № 5(33). С. 6.
5. Усцелемов В.Н. Анализ таксономии сетевых атак в распределенных информационных системах // Информационно-экономические аспекты стандартизации и технического регулирования. 2016. № 6(34). С. 4.
6. Бурый А.С., Шевкунов М.А. Интеллектуализация процессов принятия решений в эргатических системах // Транспортное дело России. 2015. № 4. С. 48-50.
7. Ловцов Д.А. Информационная теория эргасистем: Тезаурус. – М.: Наука, 2005. – 248 с.
8. Бурый А.С. Картирование технологий как метод в форсайт-исследованиях // Транспортное дело России. 2014. № 5. С. 155-157.
9. Микрюков А.А., Усцелемов В.Н. Гибридная модель оценки рисков в информационных системах // Прикладная информатика. 2014. № 1(49). С. 50-55.
10. Jalali M.S., Siegel M., Madnick S. Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment // The Journal of Strategic Information Systems. 2019. Vol. 28. No. 1, pp. 66-82.
11. Бурый А.С. Распределенные системы оценивания со случайной структурой // Автом. и телемех. 1994. № 12. С. 70-75.
12. Buczak A.L., Guven E. A survey of Data Mining and Machine Learning methods for cyber security intrusion detection // IEEE Communications Surveys & Tutorials. 2016. Vol. 18. No. 2, pp. 1153-1176.
13. Buryi A.S., Lomakin M.I., Sukhov A.V. Quality assessment of "Stress-Strength" models in the conditions of Big Data // International Journal of Innovative Technology and Exploring Engineering. 2020. No. 9(3), pp. 3276–3281.
14. Carson J. Key takeaways from the 2019 verizon data breach investigations report. [Электронный ресурс]. – Режим доступа: https://thycotic.com/company/blog/2019/05/21/
15. Олейник А.Г., Ломов П.А. Разработка онтологии интегрированного пространства знаний // Онтология проектирования. 2016. Т. 6. № 4(22). С. 465-474.
16. Массель А.Г., Гаськова Д.А. Онтологический инжиниринг для разработки интеллектуальной системы анализа угроз и оценки рисков кибербезопасности энергетических объектов // Онтология проектирования. 2019. Т. 9. № 2(32). С. 225-238.
17. Ворожцова Т.Н. Онтология как основа для разработки интеллектуальной системы обеспечения кибербезопасности // Онтология проектирования. 2014. № 4(14). С. 69-77.
18. Бурый А.С., Морин Е.В. Модельно-алгоритмические структуры оценки качества программных изделий. – М.: Горячая линия – Телеком, 2019. – 160 с.
19. Бурый А.С., Стреха А.А. Когнитивный подход к управлению организационными изменениями предприятий // Транспортное дело России. 2015. № 4. С. 3-6.

ONTOLOGICAL APPROACH TO FORMATION COGNITIVE MODELS FOR ASSESSING CYBERSECURITY

Buryi Aleksey Sergeevich, doctor of technical sciences, Director of the De-partment, FSUE STANDARTINFORM, Moscow
Ustselemov Vyacheslav Nikolaevich, applicant, FSUE STANDARTINFORM, Moscow

The issues of ensuring cybersecurity of information systems functioning in the conditions of big data caused by the growth of the number of information sources are considered.
To improve the cybersecurity of modern information systems, a methodologi-cal approach is proposed that includes: 1) analysis of cyberspace, based on the development of ontological structures of conceptual events (scenario chains of typi-cal actions) to identify cyber threats and possible dangers; 2) development of cog-nitive models for assessing the cybersecurity of information systems for the organi-zation of parrying cyber-attacks with the involvement of big data Analytics.
Cyber-ontologies are proposed to be considered as adaptive dictionaries of data, applications, and user relationships to improve behavior scenarios and anal-ysis in order to prevent the spread of threats before they occur. The considered on-tological structure allows you to systematize possible sources of threats, and take protective measures, perform monitoring of cyberspace in order to assess vulnera-bilities, and the level of risks in various combinations of threats and measures tak-en to eliminate them.
Key words: cybersecurity, cyberspace, cyber threats, knowledge structuring, ontological engi-neering, cognitive models

REFERENCES:

1. GOST R ISO/IEC 27000-2012. Informacionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Sistemy menedzhmenta informacionnoj bezopasnosti. Obshchij obzor i terminologiya. [*Information technology. Security techniques. Information security management systems. Overview and vocabulary*]. Moscow, Standartinform, 2019.
2. Markov A.S., Tsirlov V.L. Rukovodyashchie ukazaniya po kiberbezopasnosti v kontekste ISO 27032. Voprosy kiberbezopasnosti. 2014. No. 1(2), pp. 28-35.
3. GOST R ISO/IEC 27005-2010. Informacionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Menedzhment riska informacionnoj bezopasnosti [Information technology. Security techniques. Information security risk management]. Moscow, Standartinform, 2011.
4. Buryi A.S., Ustselemov V.N. Organizaciya informacionnoj bezopasnosti v avtomatizirovannyh sistemah upravleniya [*Organization of information security in the automated control systems*]. Informacionno-ekonomicheskie aspekty standartizacii i tekhnicheskogo regulirovaniya. 2016. No. 5(33). P. 6.
5. Ustselemov V.N. Analiz taksonomii setevyh atak v raspredelennyh informacionnyh sistemah [*Analysis of network attacks taxonomy in distributed information systems*]. Informacionno-ekonomicheskie aspekty standartizacii i tekhnicheskogo regulirovaniya. 2016. No. 6(34). P. 4.
6. Buryi A.S., Shevkunov M.A. Intellektualizaciya processov prinyatiya reshenij v ergaticheskih sistemah [Intellectualization of decision-making processes in ergatic systems]. Transportnoe delo Rossii. 2015. No. 4, pp. 48-50.
7. Lovtsov D.A. Informacionnaya teoriya ergasistem: Tezaurus. Moscow, Nauka, 2005. 248 p.
8. Buryi A.S. Kartirovanie tekhnologij kak metod v forsajt-issledovaniyah [*Mapping technology as a method in foresight research*]. *Transportnoe delo Rossii*. 2014. No. 5, pp. 155-157.
9. Mikryukov A.A., Ustselemov V.N. Gibridnaya model' ocenki riskov v informacionnyh sistemah. [The hybrid model of risk assessment in information systems]. Prikladnaya informatika. 2014. No. 1(49), pp. 50-55.
10. Jalali M.S., Siegel M., Madnick S. Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. The Journal of Strategic Information Systems. 2019. Vol. 28. No. 1, pp. 66-82. DOI: 10.1016/j.jsis.2018.09.003.
11. Buryi A.S. Distributed estimation systems with random structure. Avtomatika i Telemehanika. 1994. No. 12, pp. 70-75.
12. Buczak A. L., Guven E. A Survey of Data Mining and Machine Learning Methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials. 2016. Vol. 18. No. 2, pp. 1153-1176. DOI: 10.1109/COMST.2015.2494502.

13. Buryi A.S., Lomakin M.I., Sukhov A.V. Quality assessment of "Stress-Strength" models in the conditions of Big Data. International Journal of Innovative Technology and Exploring Engineering. 2020. 9(3), pp. 3276-3281. DOI: 10.35940/ijitee.C8982.019320.
14. Carson J. Key Takeaways from the 2019 Verizon Data Breach Investigations Report [Online]. – Available at: https://thycotic.com/company/blog/2019/05/21/ (accessed 28 April 2020).
15. Oleynik A.G., Lomov P.A. Razrabotka ontologii integrirovannogo prostranstva znanij. Ontologiya proektirovaniya. 2016. Vol. 6. No. 4(22), pp. 465-474. DOI: 10.18287/2223-9537-2016-6-4-465-474.
16. Massel A.G., Gaskova D.A. Ontologicheskij inzhiniring dlya razrabotki intellektual'noj sistemy analiza ugroz i ocenki riskov kiberbezopasnosti energeticheskih ob"ektov. Ontologiya proektirovaniya. 2019. Vol. 9. No. 2(32), pp. 225-238.
17. Vorozhtsova T.N. Ontologiya kak osnova dlya razrabotki intellektual'noj sistemy obespecheniya kiberbezopasnosti. Ontologiya proektirovaniya. 2014. No. 4(14), pp. 69-77.
18. Buryi A.S., Morin E.V. Modelno-algoritmicheskie struktury ocenki kachestva programmnyh izdelij [Model-algorithmic structures of software products quality assessment]. Moscow, Hotline-Telecom, 2019. 160 p.
19. Buryi A.S., Strekha A.A. Kognitivnyj podhod k upravleniyu organizacionnymi izmeneniyami predpriyatij. Transportnoe delo Rossii. 2015. No. 4, pp. 3-6.