УДК 004.056:62.50

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Бурый А.С., д-р техн. наук, директор департамента, ФГБУ «Институт стандартизации»

Усцелемов В.Н., соискатель ФГБУ «Институт стандартизации»

На примере автоматизированной системы управления технологическим процессом предложен концептуальный подход к последовательной двухуровневой структуризации сложной системы применительно к задачам информационной безопасности (ИБ). В условиях соперничества в области технологий, инноваций, возрастают требования к ИБ на различных уровнях управления в организационных системах, когда основными формами существования и проявления информации являются активные формы: преобразования, координации, управления, выработки решений, для которых актуальность понятия «защищенности» объясняется ее динамичностью. Декомпозиция функциональных задач на отдельные подсистемы позволяет упростить процесс анализа и учитывать динамику функционирования при организации информационной защиты.

Методы исследования: системный анализ задач информационной безопасности, целевой иерархии и обоснования структур построения и комплек-сирования подсистем и процессов. Цель работы – аргументировать необходимость разработки концепции многоуровневой структуризации систем для комплексного решения задач информационной безопасности на основе ключевых принципов: конфиденциальности, целостности и доступности.

Ключевые слова: информационная безопасность, автоматизированные системы управления технологическими процессами, функциональная подсистема, обобщенный типовой технологический процесс, информационная защита.

ВВЕДЕНИЕ

Уровень развития информационно-коммуникационных технологий (ИКТ) все чаще выступает определяющим фактором экономической и политической жизни общества, формирует технологический уклад в таких видах деятельности, как управление организационными процессами, социальная сфера, образование и многих других. Среди основных тенденций развития рынка отрасли информационных технологий (ИТ) – открытые ресурсы, облачная инфраструктура, увеличение числа проектов на основе искусственного интеллекта. Обеспечение информационной безопасности (ИБ) основывается на комплексности (объединении технологических решений с организационным и нормативно-правовым обеспечением) и кросс-платформенности[1] (на примере мобильных устройств возможность перехода на iOS, Android, Windows для выбранного ресурса).

Информационная технология – это прежде всего процесс, использующий совокупность средств и методов обработки, передачи, тиражирования, распространения данных (первичной информации) для получения информации иного качества (информационного продукта), например, телетекстов, видео-, аудиофайлов и др. [1].

Информационные системы объединяют технические и программные средства, информационные технологии с целью преобразования и/или переработки поступающей информации в процессе решения поставленных задач. Автоматизированные системы (АС) в контурах управления процессами и системами охватывают персонал, комплексы средств автоматизации, реализующие ИТ в ходе выполнения установленных функций[2]. АС являются частным случаем более сложных человеко-машинных систем управления – эргатических систем, применяемых для управления объектами технических, технологических, экономических, организационных и др. комплексов [1]. При этом объектами управления выступают структурно и функционально сложные, информационно-насыщенные системы и процессы, например, при навигационном обеспечении космических аппаратов [2] и в ходе управления технологическими операциями на борту летательного аппарата [1, 3], в автоматизирован-

[1] Главные тренды развития российской отрасли информационных технологий в 2022 году. [Электронный ресурс]. – URL: https://www.tadviser.ru/ (дата посещения: 11.01.2023).

[2] ГОСТ Р 59853–2021. ИТ. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. (Введ. 2022-01-01), (п. 2).

ных системах управления (АСУ) специального назначения, объединяющих информационные ресурсы в общее информационное пространство [4].

В условиях противоборства, соперничества в области технологий, инноваций возрастают требования к информационной безопасности на различных уровнях управления в организационных структурах. Это особенно актуально для обычных информационно-поисковых систем [5] и государственных информационных систем (ИС) [6], формирующих структуру информационного взаимодействия отраслевого и межотраслевого масштаба, для решения задач межотраслевой интеграции информационных технологий, в рамках стратегии развития умных городов [7], включая беспилотные транспортные средства умного города [8].

Цель работы – рассмотрение понятия «информационная безопасность» для обоснования необходимости разработки методического подхода к концепции последовательного структурирования системы на функциональные подсистемы в соответствии с технологическими процессами, а затем и ТП – на отдельные процедуры и операции для обеспечения контроля и защиты информации.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК КЛЮЧЕВОЙ ФАКТОР ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Степень уязвимости перерабатываемой информации в распределенных ИС существенно возросла вследствие:

– широкого развития систем баз данных и знаний (БДЗ), разнотипных по структуре, типу информации и содержанию;
– создания и развития глобальных телематических сетей, включая интернет, сети связи (в основном беспроводные) и др.;
– усложнения информационно-вычислительных процессов, в том числе за счет внедрения облачных сервисов;
– повышения рисков, связанных с расширением круга лиц, имеющих доступ к информационным и программно-техническим ресурсам.

Сущность ИБ раскрывают три ключевых принципа, называемых триадой *CIA*[3], которая включает понятия [1, 9]:

– **конфиденциальности** (скрытности, селективной доступности) динамической и статистической информации при несанкционированном доступе (НСД) и использовании (НСД);
– **целостности** (сохранности, готовности) статистической информации в составе информационных массивов БДЗ, необходимых для решения целевых и функциональных задач;
– доступности (прав пользования) динамической информации, включая чтение, копирование, уничтожение, изменение или переработку авторизированным сторонам.

Разрабатываемые политики ИБ должны плавно интегрировать все принципы триады CIA при оценке и внедрении новых технологий и сценариев.

Применительно к автоматизированным системам к активным формам существования информации можно отнести преобразование, координацию, управление, выработку решения, для которых на фоне динамичности наиболее актуально понятие защищенности.

В основу классификации видов ИБ предлагается положить прикладные аспекты (инструментарий) ИТ:

1. Для приложений (Бп) – это защита интерфейсов и прикладных программ; выявление возможных уязвимостей для предотвращения доступа (программным путем) к другим программным продуктам (приложениям).
2. Безопасность инфраструктуры (Би), включая сети, серверы, клиентские технические средства, центры обработки данных, так как рост числа оконечных устройств и их связности усложняет инфраструктуру, увеличивая риски уязвимости систем.
3. Облачная безопасность (Бо) – обеспечивает защиту, аналогичную безопасности приложений и инфраструктуры, но ориентирована на облачные ресурсы ИБ, и предоставляется провайдером облачных услуг.

Таким образом, под ИБ понимается свойство субъекта или объекта, характеризующее степень защищенности его потребностей и интересов в качественной информации, необходимой ему для нормального (устойчивого) функционирования (жизнедеятельности) и развития [1].

Анализ основных технологий цифровой трансформации, включая интернет вещей, большие данные, искусственный интернет, облачные вычисления, киберфизические системы, показывает, что ИБ данных технологий превращается в сигнал SOS (в плане необходимости научно-методологической поддержки данного направления), требующий комплексного подхода к организации ИБ на основе объединения перечисленных выше форматов безопасности – $Б_п$, $Б_и$, $Б_о$.

С появлением сетевых структур, внедрением интернет-технологий возможными причинами отказов и сбоев в работе оборудования стали не только его техническое состояние, но и действия другой стороны с целью несанкционированного получения информации или ее уничтожения, изменения и т. д. Это обусловило необходимость обеспечения ИБ как механизма «защиты конфиденциальности, целостности и доступности информации», а также появление систем интеллектуальных сервисов защиты информации,

[3] От Confidentiality – Integrity – Availability (пер. с англ.: конфиденциальность, целостность, доступность).

использующих технологию управления информацией и событиями безопасности [10]. Организационные и технические меры защиты информации, реализованные в рамках системы (подсистемы) защиты информации (ПЗИ), например, в АСУ технологическим процессом, должны быть направлены на исключение:

– неправомерного доступа, копирования, предоставления или распространения информации (то есть на обеспечение конфиденциальности информации);
– неправомерного уничтожения или модифицирования информации (обеспечение целостности информации);
– неправомерного блокирования информации (обеспечение доступности информации);
– конфликтной устойчивости применения информационных систем к действиям конкурирующей стороны, реализуемой методами и средствами информационной безопасности [11].

В ходе конфликтного взаимодействия может решаться задача контроля определенного типа ресурса, например, информационного, либо защиты этого ресурса за счет проведения специальных мероприятий при обеспечении эффективности функционирования защищаемой информационной системы [4]. ИС может быть представлена в виде организационно-технической системы как класса автоматизированных ресурсов, обеспечивающих выработку управляющих решений на основе автоматизированных информационных процессов в различных сферах управления, проектирования, контроля и измерения параметров, предоставления услуг или иной деятельности, осуществляемой человеком [12].

СТРУКТУРИЗАЦИЯ ПРОЦЕССОВ И СИСТЕМ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

На примере АСУ технологическим процессом (ТП) рассмотрим роль задач обеспечения ИБ. На рис. 1 представлена структурная схема взаимодействия основных подсистем (п/с) АСУ ТП, выделена подсистема защиты информации, включающая несколько уровней безопасности (условно показаны два уровня (цифры 1 и 2) – защита внутреннего и внешнего информационного контура управления). Данное представление инвариантно к объекту управления (ОУ), в качестве которого может выступать любой технологический процесс, связанный с переработкой информации под управлением поступающей управляющей информации от п/с выработки решений (ВР). Результаты контроля ОУ передаются в п/с измерений и сбора информации (ИСИ), а затем в п/с оценивания и обработки. Затем результаты вычислений поступают в организационную (Орг.) п/с, где принимается решение о состоянии ОУ (функциональном, целевом, техническом).

Применяемые средства защиты информации функционируют таким образом, что «разрешаемые ими виды доступа к ИС должны переводить ее только в безопасное состояние» [13].

Поступающее в Орг. п/с внешнее управление представляет собой целевые установки (задачи управления) от вышестоящих уровней управления, а выходные данные – это результаты управления. ПЗИ в данном случае функционирует в рамках подсистемы информационного обмена (ИО), которая обеспечивает взаимодействие указанных подсистем, ОУ и внешних систем управления между собой.

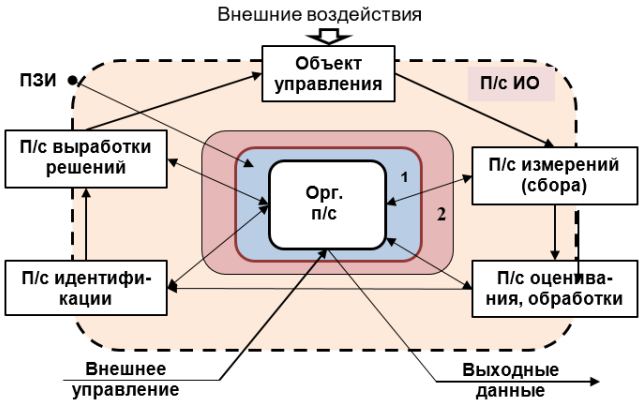

Рис. 1. Структурная схема информационного взаимодействия подсистем инвариантного контура управления АСУ ТП

ПЗИ обеспечивает совокупность «организационных мероприятий, технических, программных, программно-технических средств защиты информации (СЗИ) и средств контроля эффективности защиты информации» для недопущения случайного или целенаправленного искажения или разрушения, раскрытия или модификации информации в ИС [1]. Уровни безопасности можно соотнести со способами их осуществления (на организационном, техническом или программном уровне).

Задачи защиты информации в подсистемах АСУ ТП

НАЗВАНИЕ ПОДСИСТЕМЫ	ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ
П/с ИСИ	Контроль качества получаемой информации и защита от ошибок
П/с идентификации	Защита от ошибок преобразования и разрушающих факторов
П/с ВР	Защита управляющей информации от НСИ
Орг. п/с	Защита от ошибок людей оператора и от несанкционированных действий (НСД)
П/с ИО	Защита от искажений при передаче, НСД, НСИ
ПЗИ	Обеспечение необходимой семантической защищенности перерабатываемой информации

В таблице представлены примеры типов задач по ЗИ в различных подсистемах АСУ ТИ, изображенных на рис. 1.

Обобщенный типовой технологический процесс переработки информации при решении любой задачи в автоматизированных информационных системах представим в виде ориентированной цепи технологических операций (рис. 2), с учетом подхода [ ] и логики этапов переработки данных в АСУ ТП. Ввиду сетевой информационной структуры автоматизированной системы существует опасность потери, манипуляции информационными пакетами, циркулирующими в контуре управления, поэтому помимо функций обработки информации следует учитывать операции контроля и обобщения. Обобщение позволяет получать новые данные, как правило, меньшего объема, за счет сжатия первичной информации или любого иного динамического преобразования анализируемых данных.

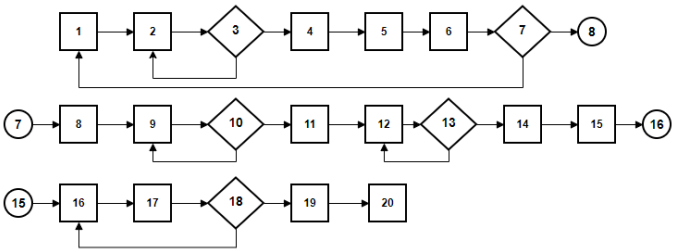

Рис. 2. Типовой технологический процесс переработки информации:

1 – обработка (сбор, регистрация исходной информации); 2 – обработка (первичное преобразование информации); 3 – контроль (определение уровня достоверности информации); 4 – обработка (классификация информации); 5 – обработка (передача информации по каналам связи); 6 – обработка (прием информации); 7 – контроль (обеспечение безопасности получаемой информации); 8 – обработка (обеспечение записи и хранения информации); 9 – обобщение (предоставление доступа пользователей к информации); 10 – контроль (проверка безошибочности входной информации); 11 – обработка (сортировка и оптимизация информационных массивов); 12 – обобщение (переработка информации в соответствии с пакетом прикладных программ); 13 – контроль (проверка адекватности полученного решения); 14 – обработка (вывод результатов для промежуточного анализа); 15 – обработка (хранение информации в БДЗ); 16 – обработка (поиск нужной информации в информационной базе); 17 – обработка (сортировка полученной информации; 18 – контроль (подготовка информации для передачи, формирование отчетов и др.); 19 – обработка (передача информации по каналам связи); 20 – обработка (отображение информации).

На фоне дестабилизирующих факторов, приводящих, в конечном счете, к выходу из строя элементов информационной системы, требуется постоянное совершенствование организации функционирования ИС, ее технической, функциональной и технологической реконфигурации [, ,]. Модели контроля, обработки, обобщения данных для своевременного оперативного выявления дестабилизирующих факторов все чаще формируются на базе новых подходов и способов решения задач оптимизации, включая многоагентные системы, генетические модели, нейронные сети. Кроме того, сочетание теории нечетких систем, нейронных сетей, вероятностных рассуждений и генетических алгоритмов дает синергетический эффект, получивший название мягких вычислений, позволяет значительно расширить возможности подсистем обнаружения вторжений и атак за счет интеллектуального анализа данных [ ], обеспечивающих комплексную защиту информации в автоматизированных системах управления.

ЗАКЛЮЧЕНИЕ

Преимущество этапа структуризации в любой исследовательской задаче позволяет понять имеющиеся ресурсы, выделить цель исследования и наметить последовательность движения к заданной цели.

Применительно к задаче исследования – обеспечение информационной безопасности любой сложной системы – предлагается декомпозировать систему (АСУ ТП) на функциональные подсистемы, выделить в них возможные уязвимости, относительно которых и строится система ИБ. На уровне выбранного ТП следует организовать (продумать) рациональное сочетание стадий обработки данных (информации) с этапами контроля информационных воздействий, угроз, с оценкой устойчивости и выработки управляющих воздействий для выполнения при необходимости динамической реконфигурации подсистемы информационной безопасности.

Дальнейшим направлением исследований видится разработка методического аппарата (методов и алгоритмов) классификации инцидентов в соответствии с текущими деструктивными воздействиями, обеспечивающими минимальное отклонение текущего состояния информационной системы от ее безопасного состояния. Это необходимо для оценки риска преодоления уровня информационной защиты и подготовки ответных мер.

Список использованных источников и литературы

1. Ловцов Д.А. Теория защищенности информации в эргасистемах: Монография. – М.: РГУП, 2022. – 276 с.
2. Алексеев О.А., Бурый А.С., Дубинко Ю.С., Сильвестров С.Д. Патент № 2125732 C1 РФ, МПК G01S 5/02. Способ навигационных определений по интегральным параметрам: № 97101751/09: заявл. 05.02.1997: опубл. 27.01.1999.
3. Бурый А.С., Шевкунов М.А. Интеллектуализация процессов принятия решений в эргатических системах // Транспортное дело России. 2015. № 4. С. 48–50.
4. Агеев С.А., Саенко И.Б. Управление безопасностью защищенных мультисервисных сетей специального назначения // Труды СПИИРАН. 2010. Вып. 2(13). С. 182–198.
5. Щекочихин О.В., Синкевич Е.А. Обеспечение информационной безопасности при работе с информационно-поисковыми системами // Информационно-экономические аспекты стандартизации и технического регулирования. 2022. № 2(66). С. 35–40.
6. Бурый А.С. Совершенствование государственных информационных систем как тренд цифрового общества // Правовая информатика. 2020. № 3. С. 19–28. https://doi.org/10.21681/1994-1404-2020-3-19-28
7. Бурый А.С., Ловцов Д.А. Информационные структуры умного города на основе киберфизических систем // Правовая информатика. 2022. № 4. С. 15–26. https://doi.org/10.21681/1994-1404-2022-4-15-26
8. Промыслов В.Г. Семенков К.В., Жарко Е.Ф. Методы оценки информационной угрозы для беспилотных транспортных средств в среде «умного города» // Проблемы управления. 2020. № 3. С. 49–58. https://doi.org/10.25728/pu.2020.3.6
9. Усцелемов В.Н. Анализ угроз информационной безопасности организационно-технических систем // Информационно-экономические аспекты стандартизации и технического регулирования. 2020. № 1(53). С. 69–76.
10. Котенко И.В., Саенко И.Б. Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. 2012. № 3(22). С. 84–100.
11. Мистров Л.Е., Кравцов Е.В. Метод представления информационных процессов в системах обеспечения информационной безопасности критически важных объектов // Информационно-экономические аспекты стандартизации и технического регулирования. 2019. № 6 (52). С. 42–47.
12. Соловьев И.В., Цветков В.Я. Принципы когнитивного управления сложной организационно-технической системой // Государственный советник. 2016. № 1. С. 27–32.
13. Еремеев М.А., Ломако А.Г. и др. Метод комбинированного доступа к информационным ресурсам в гетерогенной распределенной автоматизированной системе специального назначения // Вопросы защиты информации. 2009. № 4. С. 42–50.
14. Дружинин Г.В., Сергеева И.В. Качество информации. – М.: Радио и связь, 1990. – 172 с.
15. Buryi A. S. Structure complexity of distributed information-control systems // Izvestiya Rossiiskoi Akademii Nauk. Teoriya i Sistemy Upravleniya. 1994. No. 5. Pp. 160–167.
16. Шелухин О.И., Ерохин С.Д., Полковников М.В. Технологии машинного обучения в сетевой безопасности. – М.: Горячая линия – Телеком, 2021. – 360 с.

INFORMATION SECURITY OF AUTOMATED SYSTEMS

Buryi A.S., Dr. Sc. (Technology), Department Director at the FSBI «RSI»

Ustselemov V.N., candidate of the FSBI «RSI»

Using the example of an automated process control system, a conceptual approach of sequential two-level structuring of a complex system in the tasks of the information security paradigm is proposed. Research methods: system analysis of information security tasks, target hierarchy and justification of structures for building and integrating subsystems and processes. In the conditions of competition in the field of technology and innovation, the requirements for information security at various levels of management in organizational systems are increasing, when the main forms of existence and manifestation of information are active forms: transformation, coordination, management, decision-making, for which the relevance of the concept of "protection" is explained by its dynamism.

The decomposition of functional tasks into separate subsystems makes it possible to simplify the analysis process and take into account the dynamics of functioning when organizing information protection. The purpose of the work is to substantiate the need to develop a concept of multi-level structuring of systems for complex solutions to information security problems based on key principles: confidentiality, integrity and accessibility.

Keywords: information security, automated process control systems, functional subsystem, generalized typical technological process, information protection.

References

1. Lovtsov D.A. Teoriya zashchishchennosti informacii v ergasistemah: Monografiya. Moscow, RGUP Publ., 2022, 276 p. (In Russian).
2. Alekseev O.A., Buryi A.S., Dubinko Yu.S., Sil'vestrov S.D. Patent № 2125732 C1 RF, MPK G01S 5/02. Sposob navigacionnyh opredelenij po integral'nym parametram: № 97101751/09 : zayavl. 05.02.1997 : opubl. 27.01.1999. (In Russian).
3. Buryi A.S., Shevkunov M.A. Intellektualizaciya processov prinyatiya reshenij v ergaticheskih sistemah. Transportnoe delo Rossii. 2015, no. 4, pp. 48–50. (In Russ., abstr. in Engl.).
4. Ageev S.A., Saenko I.B. Upravlenie bezopasnost'yu zashchishchennyh mul'tiservisnyh setej special'nogo naznacheniya. Trudy SPIIRAN. 2010, no. 2(13), pp. 182–198.
5. Shchekochihin O.V., Sinkevich E.A. Obespechenie informacionnoj bezopasnosti pri rabote s informacionno-poiskovymi sistemami. Informacionno-ekonomicheskie aspekty standartizacii i tekhnicheskogo regulirovaniya. 2022, no. 2 (66), pp. 35–40. (In Russ., abstr. in Engl.).
6. Buryi A.S. Sovershenstvovanie gosudarstvennyh informacionnyh sistem kak trend cifrovogo obshchestva. Pravovaya informatika. 2020, no. 3, pp. 19–28. https://doi.org/10.21681/1994-1404-2020-3-19-286 . (In Russ., abstr. in Engl.).
7. Buryi A.S., Lovtsov D.A. Informacionnye struktury umnogo goroda na osnove kiberfizicheskih system. Pravovaya informatika. 2022, no. 4, pp. 15–26. https://doi.org/10.21681/1994-1404-2022-4-15-26 (In Russ., abstr. in Engl.).
8. Promyslov V.G. Semenkov K.V., ZHarko E.F. Metody ocenki informacionnoj ugrozy dlya bespilotnyh transportnyh sredstv v srede "umnogo goroda". Problemy upravleniya. 2020, no. 3, pp. 49–58. https://doi.org/10.25728/pu.2020.3.6 . (In Russ., abstr. in Engl.).
9. Ustselemov V.N. Analiz ugroz informacionnoj bezopasnosti organizacionno-tekhnicheskih system. Informacionno-ekonomicheskie aspekty standartizacii i tekh-nicheskogo regulirovaniya. 2020, no. 1(53), pp. 69–76. (In Russ., abstr. in Engl.).
10. Kotenko I.V., Saenko I.B. Postroenie sistemy intellektual'nyh servisov dlya zashchity informacii v usloviyah kiberneticheskogo protivoborstva. Trudy SPIIRAN. 2012, no. 3 (22), pp. 84–100. (In Russ., abstr. in Engl.).
11. Mistrov L.E., Kravtsov E.V. Metod predstavleniya informacionnyh processov v sistemah obespecheniya informacionnoj bezopasnosti kriticheski vazhnyh ob"ektov. Informacionno-ekonomicheskie aspekty standartizacii i tekhnicheskogo regulirovaniya. 2019, no. 6 (52), pp. 42–47. (In Russ., abstr. in Engl.).

12. Solov'ev I.V., Tsvetkov V.Ya. Principy kognitivnogo upravleniya slozhnoj organizacionno-tekhnicheskoj sistemoj. Gosudarstvennyj sovetnik. 2016, no. 1, pp. 27–32.
13. Eremeev M.A., Lomako A.G. i dr. Metod kombinirovannogo dostupa k informacionnym resursam v geterogennoj raspredelennoj avtomatizirovannoj sisteme special'nogo naznacheniya. Voprosy zashchity informacii. 2009, no. 4, pp. 42–50. (In Russ., abstr. in Engl.).
14. Druzhinin G.V., Sergeeva I.V. Kachestvo informacii. Moscow, Radio i svyaz', 1990, 172 p.
15. Buryi A. S. Structure complexity of distributed information-control systems. Izvestiya Rossiiskoi Akademii Nauk. Teoriya i Sistemy Upravleniya. 1994, no. 5, pp. 160–167.
16. Sheluhin O.I., Erohin S.D., Polkovnikov M.V. Tekhnologii mashinnogo obucheniya v setevoj bezopasnosti. Moscow, Goryachaya liniya – Telekom Publ., 2021, 360 p. (In Russian).