УДК 004.72:65.011.56 Вестник УрФО № 2(60) / 2026, с. 24–31

Быкасов А. В., Соколов А. Н.

DOI: 10.14529/secur260203

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ВЛИЯНИЯ АКТИВНОГО СКАНИРОВАНИЯ НА СТАБИЛЬНОСТЬ ФУНКЦИОНИРОВАНИЯ СЕТИ АСУ ТП

В статье рассматривается задача обеспечения кибербезопасности автоматизированных систем управления технологическими процессами (АСУ ТП) при применении методов активного сетевого сканирования. Предложена аналитическая математическая модель трафика промышленной сети, построенная на основе теории массового обслуживания (ТМО). Модель позволяет прогнозировать задержки при передаче данных, длину очередей сообщений и коэффициент загрузки сетевых узлов до начала проведения сканирования. Показана взаимодополняемость аналитического подхода и современных моделей доверия к методам активного сканирования. Сформулированы критерии безопасного внедрения сканирования, обеспечивающие непрерывность технологического процесса и ограничение суммарной задержки $D_{total} < 10$ мс. Установлено, что поддержание коэффициента загрузки $\rho \leq 0{,}7$ предотвращает экспоненциальный рост времени ожидания в очередях. Результаты исследования могут быть применены при проектировании регламентов кибербезопасности, планировании окон обслуживания и разработке адаптивных алгоритмов сканирования.

Ключевые слова: *АСУ ТП, теория массового обслуживания, активное сканирование, математическое моделирование, сетевой трафик, кибербезопасность, задержки передачи, коэффициент загрузки, модель доверия.*

MATHEMATICAL MODELING OF THE IMPACT OF ACTIVE SCANNING ON THE STABILITY OF THE INDUSTRIAL CONTROL NETWORK

This paper addresses the challenge of ensuring the cybersecurity of industrial control systems (ICS) when employing active scanning methods. An analytical mathematical model of industrial network traffic based on queuing theory is proposed. This model allows for prediction of data transmission delays, message queue lengths, and network node utilization rates prior to the commencement of scanning operations. The complementarity between this analytical approach and modern trust models regarding active scanning methods is demonstrated. Criteria for the safe implementation of network scanning are formulated, ensuring both the continuity of technological processes and a total delay limit of $D_{total} < 10$ ms. It is established that maintaining a utilization rate of $\rho \leq 0.7$ prevents the exponential growth of queuing wait times. The findings of this study can be applied in the design of cybersecurity protocols, the scheduling of maintenance windows, and the development of adaptive scanning algorithms.

Keywords: *ICS, queuing theory, active scanning, mathematical modeling, network traffic, cybersecurity, transmission delays, load factor, trust model.*

Обеспечение информационной безопасности автоматизированных систем управления технологическими процессами (АСУ ТП) является важной задачей для объектов критической информационной инфраструктуры (КИИ), особенно в условиях нарастающей волны целевых атак на промышленные системы. Как следствие наличия модернизируемой базы кибератак, постоянно возрастает потребность в проведении регулярной оценки уязвимостей сетевой инфраструктуры. Активное сканирование портов и служб попрежнему остается одним из самых эффективных способов выявления слабых мест, но в АСУ ТП его целесообразность подвергается сомнению по причине наличия огромного количества серьезных рисков. Избыточные запросы могут привести к перегрузке каналов связи и увеличению задержек передачи данных, а также вызвать сбои в работе программируемых логических контроллеров (ПЛК) и человеко-машинных интерфейсов (HMI).

Существующие подходы к оценке воздействия сканирования носили эмпирический характер и не учитывали возможности обеспечения необходимой надежности и безопасности результатов. В работе [1] рассматриваются основные методы активного сканирования сетей АСУ ТП и описываются алгоритмы их реализации. В результате применения методов активного сканирования была построена UML-диаграмма активов сети АСУ ТП. Сформулированы условия доверия, применимые к методам активного сканирования, которые позволят разрабатывать безопасные методы сбора и анализа сетевой информации с целью создания верифицированной системы активного сканирования для поиска уязвимостей в сетях АСУ ТП.

В работе [2] представлена статистическая модель оценки влияния комбинированного метода активного сканирования на стабильность функционирования сети АСУ ТП. Проведены эксперименты для оценки влияния активного сканирования на стабильность функционирования промышленной сети. Полученные результаты, представленные в

сравнении с результатами для распространенного инструмента сетевого сканирования Nmap, дают сделать вывод о том, что комбинированный метод активного сканирования оказывает меньшее влияние на сеть, а также обеспечивает стабильность при сканировании, тем самым не нарушая работоспособность сети АСУ ТП.

Несмотря на высокую ценность моделей доверия и статистической валидации, для продуктивного планирования окон обслуживания и нормативного регулирования интенсивности сканирования требуется аналитический аппарат. В данной работе предлагается применение теории массового обслуживания (ТМО), фундаментальные положения которой изложены в классических работах [3, 4], для построения аналитической модели трафика АСУ ТП. При выборе параметров модели учтены рекомендации по архитектуре защищенных сетей, приведенные в [7, 8], а также требования к защите информации в промышленных сетях, регламентированные в [9] и нормативных документах ФСТЭК России [10 - 12]. Проблемы комплексного обеспечения безопасности технологических сетей, отмеченные в [13], также учитываются при формировании критериев устойчивости.

Для построения математической модели рассмотрим типовую архитектуру сети промышленной системы управления со звездообразной топологией (рис. 1).

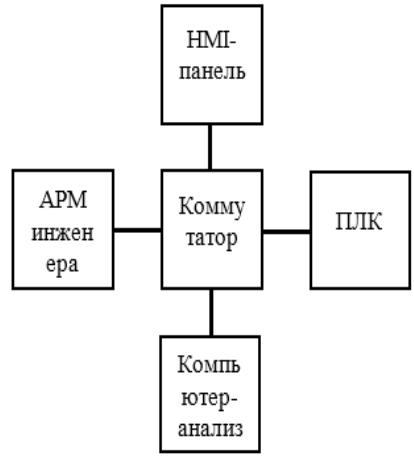

Рис. 1. Архитектура сети АСУ ТП со звездообразной топологией

Схема (рис. 1) включает следующие компоненты: HMI-панель (генерация трафика визуализации ~100 пак./с), ПЛК (обработка сенсорных данных ~50 пак./с), центральный промышленный коммутатор (пропускная способность портов 1 Гбит/с), АРМ инженера по безопасности (узел диагностики и сканирования) и сервер истории данных. Соединение осуществляется по технологии Ethernet с использованием протоколов Modbus TCP, PROFINET, Ethernet/IP, требования к безопасности которых регламентированы в [8, 9].

Трафик в сетях АСУ ТП имеет смешанный характер и делится на три основных типа, характеристики которых представлены в табл. 1.

Таблица 1

Характеристики типов трафика в сети АСУ ТП

Тип трафика	Интенсивность, пак./с	Приоритет	Распределение интервалов
Периодический (ПЛК → HMI)	50–100	Высокий	Равномерное
Событийный (аварии, алерты)	1–10 (спорадически)	Критический	Экспоненциальное
Диагностический и сканирующий	20–500 (управляемый)	Низкий	Пуассоновское

Периодический трафик характеризуется регулярной передачей данных с фиксированным интервалом $T = 1$с. Для его описания используется равномерное распределение:

$$f(t) = \begin{cases} \frac{1}{b-a}, & a \le t \le b \\ 0, & \text{иначе} \end{cases}, \qquad (1)$$

где – время ожидания между событиями,

[a, b] – интервал времени, в течение которого происходит передача пакета.

Событийный трафик возникает при аварийных ситуациях. Моделируется экспоненциальным распределением:

$$f(t) = \lambda e^{-\lambda t},\ t \ge 0, \qquad (2)$$

где t – время ожидания между аварийными событиями,

λ – интенсивность аварийных событий (среднее количество событий в единицу времени).

Диагностический и сканирующий трафик генерируется АРМ инженера и системами мониторинга сети. Характеризуется пуассонов-

ским потоком с интенсивностью , которая является управляемым параметром.

Математическая модель сетевого трафика на основе ТМО

Центральным элементом сети является коммутатор, который моделируется как система с очередями (СМО) (рис. 2). Для описания процессов поступления и обработки пакетов применяется нотация Кендалла A/B/c/K/N/D [5], где A – характер входящего потока (например, M – пуассоновский поток), B – распределение времени обслуживания одного пакета (например, M – экспоненциальное), c – количество каналов обслуживания, K – буфер очереди пакетов, N – общее количество пакетов (если очередь пакетов бесконечна, параметр опускается), D – тип обслуживания очереди пакетов (например, FIFO – первый пришел, первый обслужен).

Для базовой модели принята M/M/1,

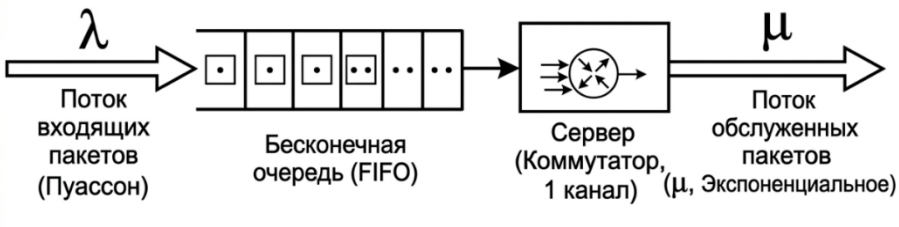

Рис. 2. Модель СМО M/M/1 для коммутатора сети АСУ ТП

предполагающая пуассоновский вход, экспоненциальное обслуживание и один канал.

Коэффициент загрузки системы:

$$\rho = \frac{\lambda}{\mu}, \quad (3)$$

где λ – интенсивность входящего потока пакетов (среднее количество пакетов в единицу времени),

μ – интенсивность обслуживания пакетов (среднее количество пакетов, которое канал может обслужить в единицу времени).

Условие стабильности: ρ < 1. Для сетей реального времени рекомендуется ρ ≤ 0,7 [6, 7].

Среднее время ожидания в очереди:

$$W_q = \frac{\rho}{\mu(1-\rho)} = \frac{\lambda}{\mu(\mu-\lambda)}. \quad (4)$$

Среднее число заявок в системе:

$$L_s = \frac{\rho}{1-\rho}. \quad (5)$$

Для АСУ ТП критически важно обеспечение приоритетной обработки технологического трафика. В модели M/M/1 с двумя классами приоритетов среднее время ожидания для технологического (высший приоритет) и сканирующего (низший приоритет) трафика определяется соответственно формулами:

$$W_q^{(1)} = \frac{1}{\mu(1-\rho_1)}, \quad (6)$$

$$W_q^{(2)} = \frac{1}{\mu(1-\rho_1)(1-\rho_1-\rho_2)}, \quad (7)$$

где $\rho_1 = \frac{\lambda_{tech}}{\mu}, \rho_2 = \frac{\lambda_{scan}}{\mu}$.

Формула (7) демонстрирует, что при приближении $\rho_1 + \rho_2$ к 1, задержки сканирующего трафика возрастают экспоненциально, не влияя на критический технологический обмен.

Расчетная модель задержек и критерии безопасности

Общая задержка передачи пакета складывается из нескольких компонент [4, 5]:

$$D_{total} = D_{trans} + D_{prop} + D_{proc} + W_q, \quad (8)$$

где D_{trans} = L/R – задержка передачи, D_{prop} = = d/v – задержка распространения, D_{proc} – задержка обработки коммутатором (10–50 мкс), W_q – очередная задержка. Требования к максимальным задержкам в промышленных сетях (D_{total} < 10 мс) соответствуют рекомендациям [8, 9].

Результаты расчета параметров сети при различной интенсивности сканирования представлены в табл. 2.

По графику можно заметить, что зависимость W_q от ρ при ρ > 0,7 имеет нелинейный характер (рис. 3), причем найденные пороговые значения кореллируют с результатами статистического моделирования [2], где экспериментально показано, что комбинированный метод активного сканирования выдает выборочное математическое ожидание для среднего показателя всплесков трафика на порядок ниже, чем метод Nmap. Это доказывает, что при условии ρ ≤ 0,7 и использовании комбинированных методов активного сканирования гарантируется предсказуемость поведения сети и отсутствие критических перегрузок.

Разработаны три критерия на основании условий доверия из [1] и нормативной базы [10 - 12], с помощью которых можно сформулировать требований безопасности для методов активного сканирования:

Таблица 2

Параметры сети при различной интенсивности сканирования

λ_{scan}, пак./с	ρ	W_q, мкс	D_{total}, мс	Статус
0	0,006	0,024	0,151	Безопасно
5000	0,206	1,03	0,116	Безопасно
10000	0,406	2,71	0,128	Безопасно
17350	0,700	9,33	0,244	Граница (ρ = 0,7)
22000	0,886	20,75	0,147	Опасно

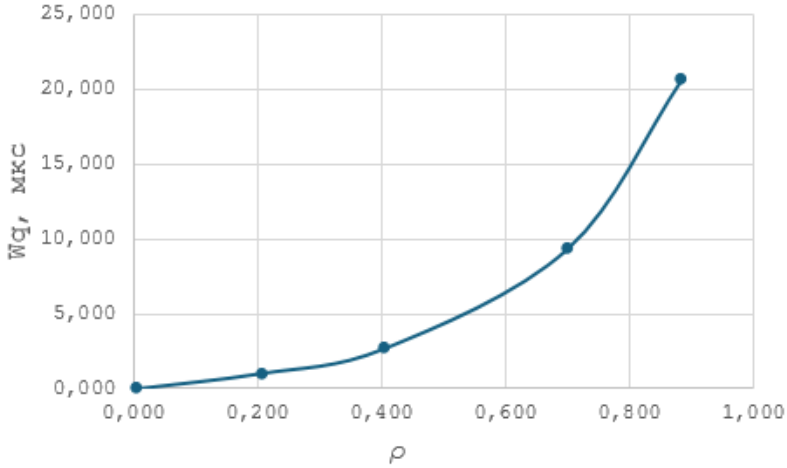

Рис. 3. Зависимость среднего времени ожидания от коэффициента загрузки

1. Непрерывность работы: вероятность отказа системы с ограниченным размером буфера очереди пакетов K, согласно (11):

$$P_{\text{отказа}} = \frac{(1-\rho)\rho^K}{1-\rho^{K+1}} < 10^{-6}, \quad (9)$$

при K = 100, что соответствует требованиям надежности промышленных сетей.

2. Минимизация нагрузки: в соответствии с первым условием доверия [1], метод активного сканирования должен исключить передачу избыточных данных:

$$\lambda_{\text{tech}} + 0_{\text{scan}} \leq 0{,}7 \cdot \mu. \quad (10)$$

3. Контроль нагрузки на устройства:

$$U_{PLC} = \frac{\lambda_{in}+\lambda_{out}}{f_{CPU}} \times 100\% < 70\%. \quad (11)$$

4. Интегральный показатель безопасности сети формируется по формуле:

$$S = w_1 \cdot \frac{D_{max} - D_{total}}{D_{max}} + w_2 \cdot \frac{0{,}7-\rho}{0{,}7} + w_3 \cdot (1 - P_{\text{отказа}}), \; S \geq 0{,}7. \quad (12)$$

В соответствии с моделью доверия, представленной в [1], для получения безопасного взаимодействия методов активного сканирования с сетями АСУ ТП необходимо выполнение трех условий доверия:

1. Исключение избыточного трафика: метод не должен создавать стабильный избыточный трафик объемом более половины минимальной полосы пропускания устройства. В терминах ТМО это условие формулируется как ограничение на интенсивность сканирующего потока:

$$\lambda_{scan} \leq \frac{Cmin}{2L_{avg}}, \quad (13)$$

где C_{min} – минимальная пропускная способность канала, L_{avg} – средний размер пакета.

2. Эффективное построение топологии сети: методология должна иметь алгоритм, позволяющий идентифицировать все включенные в сеть узлы. В соответствии с моделью ТМО условием достижения полноты построения топологической карты сети при минимальной интенсивности сканирования будет требование формулы определения вероятности

$$P_{\text{detect}} = 1 - e^{-\lambda\text{scan} \cdot \text{Tscan}} \geq 0{,}99, \quad (14)$$

которой удовлетворяет время T_{scan}, отводимое на сканирование сегмента сети.

3. Совместимость с устройствами АСУ ТП: методология должна подбирать запрос, подходящий для конкретного узла и не нарушающий его работоспособность. Реализация условия обеспечивается приоритизацией тра-

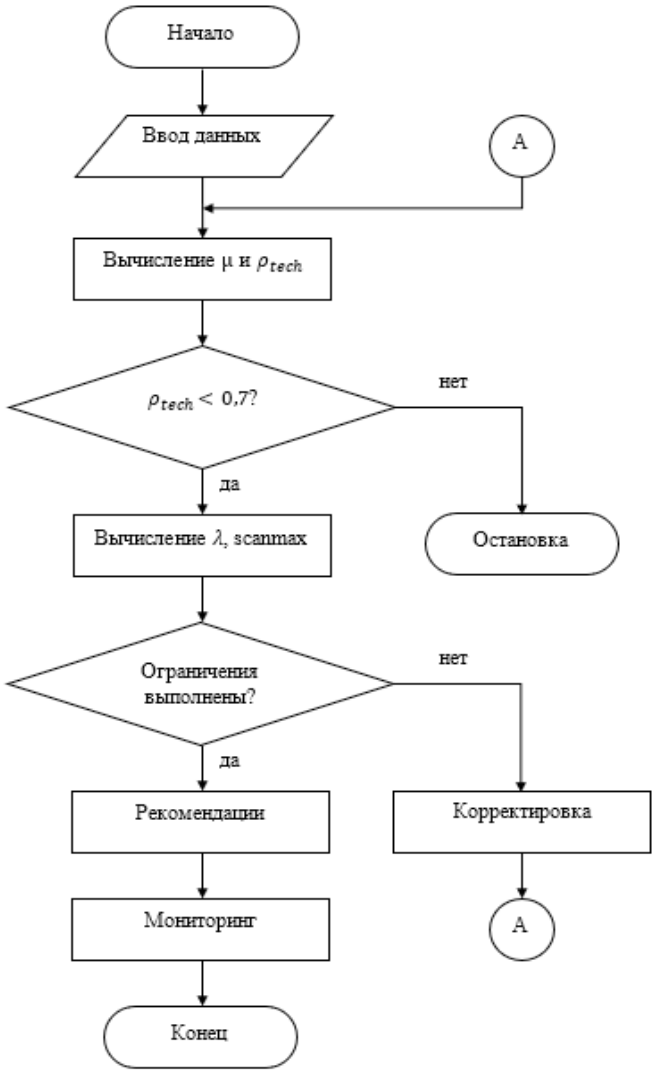

Рис. 4. Алгоритм расчета безопасных параметров сканирования

фика и адаптивным контролем интенсивности сканирования:

$$\lambda_{scan}(t) = \begin{cases} \lambda_{min}, & \rho < 0{,}5 \\ \lambda_{min} + k \cdot (0{,}7 - \rho), & 0{,}5 \le \rho \le 0{,}7 \\ 0, & \rho > 0{,}7 \end{cases} \quad (15)$$

Алгоритм расчета безопасных параметров сканирования (рис. 4) использует следующие шаги:

1) Сбор входных параметров (λ_{tech}, C, D_{max}).

2) Расчет пропускной способности $\mu = \frac{C}{L_{avg}}$ и коэффициента загруженности ρ_{tech}, проверка условия $\rho_{tech} < 0{,}7$.

3) Определение резерва по интенсивности сканирования $\lambda_{scan}^{max} = (0{,}7 - \rho_{tech})\mu$.

4) Проверка ограничений по среднему времени ожидания W_q и общей задержки передачи пакета D_{total} с использованием формул (4)–(8).

5) Формирование рекомендаций и временных окон для использования активного сканирования.

6) Мониторинг промышленной сети в реальном времени с адаптивным корректированием интенсивности трафика сканирования λ_{scan}.

Использование теории массового обслуживания для моделирования трафика АСУ ТП предоставляет строгую математическую базу для оценивания безопасности методов активного сетевого сканирования. Выявлено, что выполнение $\rho \le 0{,}7$ и $D_{total} < 10$ мс гарантирует сохранение непрерывности сетевого взаимодействия устройств промышленной сети. Аналитические результаты согласуются с современными моделями доверия [1] и статистическими моделями оценки влияния активного сканирования [2], которые подтверждают, что комбинированные методы

Таблица 3

Уровни интенсивности мониторинга промышленной сети и действия при превышении порогов

Уровень	p	D_{total}	Действие
Нормальный	<0,5	<1 мс	Продолжение сканирования
Предупреждение	0,5–0,7	1–5 мс	Снижение λ_{scan} на 25%
Тревога	0,7–0,85	5–10 мс	Снижение λ_{scan} на 50%
Критический	> 0,85	> 10 мс	Аварийная остановка сканирования

активного сканирования с управляемой интенсивностью гарантируют стабильность сети АСУ ТП при минимальных задержках внутри сети.

Разработанный алгоритм (рис. 4) и интегральный критерий безопасности (формула 12) могут быть внедрены в системы управления инцидентами (SIEM) и в оркестраторы безопасности (SOAR) для автоматизированного планирования окон анализа уязвимостей. Имеющимися перспективами исследований являются экспериментальная верификация модели на тестовых стендах с реальным промышленным оборудованием, учет приоритетной дисциплины обслуживания (Priority Queuing) и интеграция с имитационным моделированием (OMNeT++, NS-3) для верификации применяемых методов активного сканирования в условиях гетерогенных промышленных протоколов.

Литература

1. Bykasov A. V., Sokolov A. N., Barinov A. E. Trust Conditions for Active Scanning Methods for Finding Vulnerabilities in ICS Networks // 2023 International Russian Automation Conference (RusAutoCon). IEEE, 2023. DOI: 10.1109/RusAutoCon58002.2023.10272827.

2. Быкасов А. В., Соколов А. Н. Статистическая модель оценки влияния комбинированного метода активного сканирования на стабильность функционирования сети АСУ ТП // Вестник УрФО. Безопасность в информационной сфере. 2024. № 2(52). С. 68–76. DOI: 10.14529/secur240207.

3. Клейнрок Л. Теория массового обслуживания. – М.: Машиностроение, 1979. – 432 с.

4. Бронштейн О.И., Духовный И.М. Модели приоритетного обслуживания в информационно-вычислительных системах. – М.: Наука, 1976. – 220 с.

5. Гнеденко Б.В., Коваленко И.Н. Введение в теорию массового обслуживания. – 2-е изд. – М.: Наука, 1987. – 336 с.

6. Bertsekas D., Gallager R. Data Networks. – 2nd ed. – Prentice Hall, 1992. – 640 p.

7. Столлингс В. Современные компьютерные сети. – 4-е изд. – СПб.: Питер, 2021. – 784 с.

8. ENISA. Good Practices For Supply Chain Cybersecurity. – European Union Agency for Cybersecurity, 2023. – 98 p.

9. ГОСТ Р МЭК 62443-3-3-2016. Безопасность систем промышленной автоматизации. Требования к системам и компонентам. – М.: Стандартинформ, 2016.

10. Гайдмака В.А. Кибербезопасность автоматизированных систем управления технологическими процессами. – М.: Горячая линия – Телеком, 2020. – 312 с.

11. Васильев В. И., Кириллова А. Д., Кухарев С. Н. Кибербезопасность автоматизированных систем управления промышленных объектов (современное состояние, тенденции) // Вестник УрФО. Безопасность в информационной сфере. 2018. № 4(30). С. 66–74. DOI: 10.14529/secur180410.

12. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

13. Федеральный закон от 19 июля 2017 г. № 187 «О безопасности критической информационной инфраструктуры Российской Федерации».

References

1. Bykasov A. V., Sokolov A. N., Barinov A. E. Trust Conditions for Active Scanning Methods for Finding

Vulnerabilities in ICS Networks // 2023 International Russian Automation Conference (RusAutoCon). IEEE, 2023. DOI: 10.1109/RusAutoCon58002.2023.10272827.

2. Bykasov A. V., Sokolov A. N. Statisticheskaya model' otsenki vliyaniya kombinirovannogo metoda aktivnogo skanirovaniya na stabil'nost' funktsionirovaniya seti ASU TP // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. 2024. № 2(52). S. 68–76. DOI: 10.14529/secur240207.

3. Kleynrok L. Teoriya massovogo obsluzhivaniya. – M.: Mashinostroyeniye, 1979. – 432 s.

4. Bronshteyn O.I., Dukhovnyy I.M. Modeli prioritetnogo obsluzhivaniya v informatsionno-vychislitel'nykh sistemakh. – M.: Nauka, 1976. – 220 s.

5. Gnedenko B.V., Kovalenko I.N. Vvedeniye v teoriyu massovogo obsluzhivaniya. – 2-ye izd. – M.: Nauka, 1987. – 336 s.

6. Bertsekas D., Gallager R. Data Networks. – 2nd ed. – Prentice Hall, 1992. – 640 p.

7. Stollings V. Sovremennyye komp'yuternyye seti. – 4-ye izd. – SPb.: Piter, 2021. – 784 s.

8. ENISA. Good Practices For Supply Chain Cybersecurity. – European Union Agency for Cybersecurity, 2023. – 98 p.

9. GOST R MEK 62443-3-3-2016. Bezopasnost' sistem promyshlennoy avtomatizatsii. Trebovaniya k sistemam i komponentam. – M.: Standartinform, 2016.

10. Gaydmaka V.A. Kiberbezopasnost' avtomatizirovannykh sistem upravleniya tekhnologicheskimi protsessami. – M.: Goryachaya liniya – Telekom, 2020. – 312 s.

11. Vasil'yev V. I., Kirillova A. D., Kukharev S. N. Kiberbezopasnost' avtomatizirovannykh sistem upravleniya promyshlennykh ob"yektov (sovremennoye sostoyaniye, tendentsii) // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. 2018. № 4(30). S. 66–74. DOI: 10.14529/secur180410.

12. Prikaz FSTEK Rossii ot 25 dekabrya 2017 g. № 239 «Ob utverzhdenii trebovaniy po obespecheniyu bezopasnosti znachimykh ob"yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii».

13. Federal'nyy zakon ot 19 iyulya 2017 g. № 187 «O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii».

СОКОЛОВ Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой «Защита информации» федерального государственного автономного образовательного учреждения высшего образования «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, Уральский федеральный округ, Челябинская область, г. Челябинск, просп. В.И. Ленина, д. 76. E-mail: sokolovan@susu.ru

БЫКАСОВ Андрей Витальевич, аспирант федерального государственного автономного образовательного учреждения высшего образования «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, Уральский федеральный округ, Челябинская область, г. Челябинск, просп. В.И. Ленина, д. 76. E-mail: andreybikasov@gmail.com

SOKOLOV Alexander Nikolaevich, Candidate of Technical Sciences, Associate Professor, Head of the Information Security Department of the Federal State Autonomous Educational Institution of Higher Education South Ural State University (National Research University). 454080, Ural Federal District, Chelyabinsk Region, Chelyabinsk, prosp. IN AND. Lenina, d. 76. E-mail: sokolovan@susu.ru

BYKASOV Andrey Vitalievich, post-graduate student of the Federal State Autonomous Educational Institution of Higher Education "South Ural State University (National Research University)". 454080, Ural Federal District, Chelyabinsk Region, Chelyabinsk, prosp. IN AND. Lenina, d. 76. E-mail: andreybikasov@gmail.com