ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE REPUBLIC OF KAZAKHSTAN

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

2024 (19) 3

шілде - қыркүйек

ISSN 2708–2032 (print)
ISSN 2708–2040 (online)

Халықаралық ақпараттық және коммуникациялық технологиялар журналы
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Меншіктенуші: «Халықаралық ақпараттық технологиялар университеті» АҚ (Алматы қ.).
Қазақстан Республикасы Ақпарат және әлеуметтік даму министрлігінің Ақпарат комитетінде – **20.02.2020** жылы берілген.
№ KZ82VPY00020475 мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: ақпараттық технологиялар, әлеуметтік-экономикалық жүйелерді дамытудағы цифрлық технологиялар, ақпараттық қауіпсіздік және коммуникациялық технологияларға арналған.
Мерзімділігі: жылына 4 рет.
Тиражы: 100 дана
Редакцияның мекенжайы: 050040, Алматы қ-сы, Манас к-сі, 34/1, 709-кабинет, тел: +7 (727) 244-51-09.
E-mail: ijict@iitu.edu.kz Журнал сайты: https://journal.iitu.edu.kz

Международный журнал информационных и коммуникационных технологий
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Собственник: АО «Международный университет информационных технологий» (г. Алматы).
Свидетельство о постановке на учет периодического печатного издания в Министерство информации и общественного развития Республики Казахстан **№ KZ82VPY00020475,** выданное от **20.02.2020 г.**
Тематическая направленность: информационные технологии, информационная безопасность и коммуникационные технологии, цифровые технологии в развитии социо-экономических систем**.**
Периодичность: 4 раза в год.
Тираж: 100 экземпляров.
Адрес редакции: 050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09.
E-mail: ijict@iitu.edu.kz Сайт журнала: https://journal.iitu.edu.kz

«International Journal of Information and Communication Technologies»
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Owner: International Information Technology University JSC (Almaty).
The certificate of registration of a periodical printed publication in the Ministry of Information and Social Development of the Republic of Kazakhstan, Information Committee No. KZ82VPY00020475, issued on 20.02.2020.
Thematic focus: information technology, digital technologies in the development of socio-economic systems, information security and communication technologies
Periodicity: 4 times a year.
Circulation: 100 copies.
Editorial address: 050040. Manas st. 34/1, Almaty. +7 (727) 244-51-09. E-mail: ijict@iitu.edu.kz
Journal website: https://journal.iitu.edu.kz

МАЗМҰНЫ

АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАРҒА АРНАЛҒАН

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

INFORMATION TECHNOLOGY

INFORMATION SECURITY AND COMMUNICATION TECHNOLOGIES

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАРҒА АРНАЛҒАН

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

INFORMATION SECURITY AND COMMUNICATION TECHNOLOGIES

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 5. Is. 3. Number 19 (2024). Pp. 99–114
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2024.19.3.009

DEVELOPMENT OF METHODS FOR ENSURING THE SECURITY OF INDUSTRIAL AUTOMATION AND CONTROL NETWORKS AT ENTERPRISES

N.T. Duzbayev, A. Makeyev*, Y.Y. Ospanov
International Information Technology University , Almaty, Kazakhstan.
E-mail: 36169@iitu.edu.kz

Duzbayev Nurzhan Tokkuzhaevich — PhD, International Information Technology University, Almaty, Kazakhstan
E-mail: n.duzbayev@iitu.edu.kz, https://orcid.org/0000-0002-7989-9463;
Alibek Makeyev — Master's student,Computer Systems and Software Engineering, International In-formation Technology University, Almaty, Kazakhstan
E-mail: 36169@iitu.edu.kz, https://orcid.org/0009-0001-5174-825X;
Ospanov Yerlan Yerzhanovich, **—** PhD, First Deputy Head of the NSC ACADEMY
E-mail: acade-my@knb.kz, https://orcid.org/0009-0002-9256-9909.

Abstract. In the context of modern high demands on the efficiency and reliability of production processes, the security of industrial automation and control networks is becoming extremely important. This article is devoted to the research and development of methods for ensuring the security of industrial automation and control networks at enterprises, especially in the view of the growing threat of cyberattacks and other risks. The main objective of the work is to characterize industrial networks, their features and characteristics that affect approaches to ensuring security. The main threats are considered, including cyberattacks, physical interference and human errors, as well as their potential consequences for production. The authors develop and document methods for ensuring the security of industrial automation and control networks at enterprises. This includes analyzing current threats, identifying vulnerabilities and developing comprehensive solutions to protect industrial automation and control networks from various types of attacks and risks, as well as recommendations for their implementation and support. The results of the study emphasize the need for a comprehensive approach to ensuring security, and continuous monitoring and adaptation to new threats in a rapidly changing cyberspace. The project is aimed for specialists in the field of industrial

automation and information security, as well as business leaders who are interested in protecting their production systems.

Keywords: industrial automation, security, control networks, cyber threats, protection methods, network segmentation, access control

For citation: *N.T. Duzbayev, A. Makeyev, Y.Y. Ospanov. DEVELOPMENT OF METHODS FOR ENSURING THE SECURITY OF INDUSTRIAL AUTOMATION AND CONTROL NETWORKS AT ENTERPRISES // INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES. 2024. Vol. 5. No. 19. Pp. 99–114 (In Russ.). https://doi.org/10.54309/IJICT.2024.19.3.009.*

КӘСІПОРЫНДАРДАҒЫ ӨНДІРІСТІК АВТОМАТТАНДЫРУ ЖӘНЕ БАСҚАРУ ЖЕЛІЛЕРІНІҢ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІН ӘЗІРЛЕУ

Н.Т. Дузбаев, А. Макеев*, Е.Е. Оспанов
Международный университет информационных технологий, Алматы, Казахстан.
E-mail: 36169@iitu.edu.kz

Дузбаев Нуржан Токкужаевич — PhD, Халықаралық ақпараттық технологиялар университеті, Алматы, Казахстан
E-mail: n.duzbayev@iitu.edu.kz, https://orcid.org/0000-0002-7989-9463;
Алибек Макеев — магистрант ОП «Вычислительная техника и программное обеспечение», Международный университет информационных технологий, Алматы, Казахстан
E-mail: 36169@iitu.edu. kz, https://orcid.org/0009-0001-5174-825X;
Оспанов Еран Ержанұлы — PhD, ҰҚК академиясының 1 орынбасары бастығы
E-mail: acade-my@knb.kz, https://orcid.org/0009-0002-9256-9909.

Аннотация. Өндірістік процестердің тиімділігі мен сенімділігіне бүгінгі күннің жоғары талаптарымен өнеркәсіптік автоматтандыру және басқару желілерінің қауіпсіздігі өте маңызды болды. Бұл жоба кәсіпорындардағы өнеркәсіптік автоматтандыру және басқару желілерінің қауіпсіздігін қамтамасыз ету әдістерін зерттеуге және әзірлеуге арналған, әсіресе кибершабуылдар мен басқа да тәуекелдердің өсіп келе жатқан қаупі жағдайында. Жұмыстың негізгі мақсаты - өндірістік желілерді, олардың ерекшеліктері мен қауіпсіздік тәсілдеріне әсер ететін сипаттамаларын сипаттау. Кибершабуылдар, физикалық кедергілер және адам қателері және олардың өндіріске ықтимал әсері сияқты негізгі қауіп-қатерлер қарастырылады. Бұл жұмыстың негізгі мақсаты кәсіпорындардағы өнеркәсіптік автоматтандыру және басқару желілерінің қауіпсіздігін қамтамасыз ету әдістерін әзірлеу және құжаттау болып табылады. Бұл ағымдағы қауіптерді талдауды, осалдықтарды анықтауды және өнеркәсіптік автоматтандыруды және басқару желілерін әртүрлі шабуылдар мен тәуекелдерден қорғау үшін кешенді шешімдерді әзірлеуді, сондай-ақ оларды енгізу және қолдау бойынша ұсыныстарды қамтиды. Зерттеу нәтижелері қауіпсіздікке кешенді көзқарас, сондай-ақ жылдам өзгеретін киберкеңістікте жаңа қауіптерге тұрақты мониторинг және бейімделу қажеттілігін көрсетеді. Жоба өнеркәсіптік автоматтандыру және ақпараттық қауіпсіздік саласындағы мамандарға, сондай-ақ олардың өндірістік

жүйелерін қорғауға мүдделі бизнес-менеджерлерге бағытталған.

Түйін сөздер: өнеркәсіптік автоматтандыру, қауіпсіздік, басқару желілері, киберқауіптер, қорғау әдістері, желіні сегменттеу, қол жеткізуді басқару

Дәйексөз үшін: *Н. Дузбаев, А. Макеев, Е.Е. Оспанов. КӘСІПОРЫНДАРДАҒЫ ӨНДІРІСТІК АВТОМАТТАНДЫРУ ЖӘНЕ БАСҚАРУ ЖЕЛІЛЕРІНІҢ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІН ӘЗІРЛЕУ//ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ. 2024. Т. 5. No. 19. 99–114 бет. (орыс тілінде). https://doi.org/10.54309/IJICT.2024.19.3.009.*

РАЗРАБОТКА МЕТОДОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ СЕТЕЙ АВТОМАТИЗАЦИИ И УПРАВЛЕНИЯ НА ПРЕДПРИЯТИЯХ

Н.Т. Дузбаев, А. Макеев*, Е.Е. Оспанов
Международный университет информационных технологий, Алматы, Казахстан.
E-mail: 36169@iitu.edu.kz

Дузбаев Нуржан Токкужаевич — PhD, Международный университет информационных техно-логий, Алматы, Казахстан
E-mail: n.duzbayev@iitu.edu.kz, https://orcid.org/0000-0002-7989-9463;
Алибек Макеев — магистрант ОП «Вычислительная техника и программное обеспечение», Международный университет информационных технологий, Алматы, Казахстан
E-mail: 36169@iitu.edu. kz, https://orcid.org/0009-0001-5174-825X;
Оспанов Ерлан Ержанович, **—** PhD, первый заместитель начальника АКАДЕМИИ КНБ
E-mail: academy@knb.kz, https://orcid.org/0009-0002-9256-9909.

Аннотация. В условиях современных высоких требований к эффективности и надежности производственных процессов безопасность промышленной автоматизации и сетей управления становится чрезвычайно важной. Этот проект посвящен исследованию и разработке методов обеспечения безопасности промышленной автоматизации и сетей управления на предприятиях, особенно в условиях растущей угрозы кибератак и других рисков. Основной целью работы является характеристика промышленных сетей, их особенностей и характеристик, влияющих на подходы к обеспечению безопасности. Рассматриваются основные угрозы, включая кибератаки, физическое вмешательство и человеческие ошибки, а также их потенциальные последствия для производства. Авторы разрабатывают и документируют методы обеспечения безопасности промышленной автоматизации и сетей управления на предприятиях. Это включает в себя анализ текущих угроз, выявление уязвимостей и разработку комплексных решений для защиты сетей промышленной автоматизации и управления от различных типов атак и рисков, а также рекомендаций по их внедрению и поддержке. Результаты исследования подчеркивают необходимость комплексного подхода к обеспечению безопасности, а также постоянного мониторинга и адаптации к новым угрозам в быстро меняющемся киберпространстве. Проект ориентирован на специалистов в области промышленной автоматизации и информационной безопасности, а также руководителей бизнеса, которые заинтересованы в защите своих производственных систем.

Ключевые слова: промышленная автоматизация, безопасность, сети управле-

ния, киберугрозы, методы защиты, сегментация сети, контроль доступа.

***Для цитирования**: Н.Т. Дузбаев, А. Макеев, Е.Е. Оспанов. РАЗРАБОТКА МЕТОДОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ СЕТЕЙ АВТОМАТИЗАЦИИ И УПРАВЛЕНИЯ НА ПРЕДПРИЯТИЯХ// МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ. 2024. Т. 5. No. 19. Стр. 99–114. (На русс.). https://doi.org/10.54309/IJICT.2024.19.3.009.*

Введение

Выбор темы «Разработка методов обеспечения безопасности промышленных сетей автоматизации и управления на предприятиях» обусловлен растущими вызовами и потребностями в области защиты критически важных производственных систем в контексте современного технологического развития. Промышленная автоматизация и управляющие сети играют ключевую роль в ведении бизнеса, управлении технологическими процессами, обеспечении контроля и мониторинга производственных операций. Однако с ростом сложности и степени интеграции с корпоративными ИТ-системами возрастает и риск возникновения угроз, которые могут нарушить функционирование этих систем.

Задачи работы:

- Изучить структуру и элементы сетей промышленной автоматизации и управления, включая используемое оборудование и программное обеспечение;- Определить ключевые особенности и требования к безопасности, которые отличают промышленные сети от корпоративных.

Выявление и оценка угроз безопасности:

- Проанализируйте основные угрозы и уязвимости, связанные с PSA, такие как кибератаки, физическое вмешательство и человеческий фактор; Оцените потенциальное воздействие этих угроз на функционирование и безопасность производственных процессов.

В статье анализируются основные методы обеспечения безопасности, такие как сегментация сети, контроль доступа, шифрование данных, мониторинг и анализ, обновление программного обеспечения и внесение исправлений, а также физическая безопасность. Подробно рассматриваются практические аспекты внедрения этих методов и их интеграции в существующие системы промышленной автоматизации и сети управления.

Проект включает в себя обзор современных решений и технологий, а также рекомендации по их внедрению для повышения безопасности промышленных сетей. Важная роль также отводится обучению персонала и разработке политик безопасности, что позволяет нам создавать комплексный подход к защите промышленных систем.

В современном промышленном производстве автоматизация и управление играют ключевую роль в обеспечении эффективности и стабильности процессов. Сети промышленной автоматизации и управления включают в себя оборудование и программное обеспечение, которые обеспечивают контроль, мониторинговое и управляющее управление технологическими процессами. Однако с ростом взаимосвязанности и интеграции различных систем возрастает и риск возникновения угроз безопасности. Важность промышленной и управленческой безопасности возрастает в связи с потенциальными кибератаками, которые могут привести к серьезным последствиям, таким как сбои в производстве, ущерб окружающей среде или даже угроза жизни персонала. В данной статье рассматриваются основные методы

обеспечения безопасности промышленных сетей, их характеристики и практическое применение. Предметом исследования являются методы и технологии обеспечения безопасности промышленной автоматизации и сетей управления. Это включает в себя: разработку и внедрение мер по защите от киберугроз. Технологии и протоколы для обеспечения защиты данных и систем. Подходы к сегментации сети, контролю доступа, шифрованию данных и мониторингу безопасности. Методы защиты от естественных помех и человеческих ошибок. Предмет исследования: предметом исследования является промышленная автоматизация и сети управления на предприятиях. Сюда входят: инфраструктура и компоненты промышленной автоматизации и сетей управления, такие как контроллеры, датчики, исполнительные механизмы и системы управления. Сетевые протоколы и каналы связи, используемые в сетях промышленной автоматизации и управления.

Процессы и системы, которые взаимодействуют с промышленными сетями автоматизации и управления, включая корпоративные IT-системы и облачные платформы.

Методологии и практики обеспечения безопасности, применяемые в контексте промышленных сетей автоматизации и управления.

Таким образом, исследование сосредоточено на разработке и оценке методов безопасности, направленных на защиту сложных и критически важных промышленных сетей автоматизации и управления, с целью обеспечения их надежности, защиты от угроз и минимизации рисков для предприятия.

Материалы и методы исследования

Изучение международных и национальных стандартов, таких как ISO/IEC 27001, IEC 62443, NIST Cybersecurity Framework, которые определяют требования и лучшие практики для обеспечения безопасности промышленных сетей. Научные статьи и монографии: Анализ научных публикаций, посвященных современным методам и технологиям защиты промышленных сетей, а также тенденциям в области кибербезопасности и автоматизации.

Результаты

На сегодняшний день специалисты отмечают увеличение числа специалистов, обладающих современными навыками в области автоматизации зданий, и реализацию множества проектов в этой области. В то же время существует осознание необходимости перехода на новые стандарты.

В области информационных технологий необходимость защиты от киберугроз больше не ставится под сомнение. Эта потребность становится все более актуальной для промышленных систем управления. Успешная кибератака на такую систему может привести к значительным производственным потерям, нарушениям безопасности и ущербу окружающей среде, а также к утечке интеллектуальной собственности (Афонин и др., 2019). Промышленные сети, работающие непрерывно и в соответствии со строгими правилами, часто игнорируют многие политики безопасности, применимые к информационным сетям.

Ранее основной причиной защиты промышленных сетей считался человеческий фактор или сбои в их работе. В результате автоматизированное оборудование было разработано без учета риска нежелательного или неподходящего сетевого трафика. Угрозы кибератак, особенно международного характера, нацеленных на промышленные системы, практически игнорировались.

Совсем недавно в системах управления, которые не имели прямого доступа к информационным сетям компании и Интернету, использовались закрытые протоколы передачи данных. Это обеспечило безопасность промышленной сети за счет ее изоляции. Однако за последние 10–20 лет произошел переход от запатентованных технологий и стандартов к коммерчески доступным решениям в промышленных сетях (Баранова и др., 2020). Необходимость получения технологических данных из Интернета требует подключения технологических сетей к информационным системам и глобальной сети. Современные технологические сети требуют постоянного удаленного доступа и обновления данных, что делает невозможным их изоляцию. Например, промышленный Ethernet стал стандартом в области технологических коммуникаций. Аппаратное обеспечение теперь использует протоколы на основе IP, включая TCP / IP и UDP, унаследовав их уязвимости. В связи с необходимостью интеграции систем управления производством (SCADA/DMS) с высокоуровневыми ERP/MES-системами изолированность промышленной сети утратила свое значение. Кроме того, необходимо учитывать возможность проникновения вредоносных программ через интерфейсы удаленного управления и USB-порты рабочей станции, что увеличивает риски для безопасности.

Конечные устройства в технологической сети (контроллеры) были разработаны с акцентом на высокую надежность. Однако средства защиты от несанкционированного доступа к ним сегодня находятся на начальном уровне и не могут противостоять современным киберугрозам, требуя совершенствования. Использование методов кибербезопасности IT-сетями не всегда возможно из-за различий в архитектуре, типах оборудования, схемах трафика, внешних условиях и установленных правилах (Бирюков, 2020). Спектр угроз также меняется. Появление специфических промышленных вредоносных программ требует использования специализированных методов и средств защиты. Поэтому важно использовать решения, разработанные специально для промышленного сектора.

Сейчас можно утверждать, что сформировалось новое научное направление — безопасность промышленных сетей. В связи с этим было проведено исследование многих уязвимостей промышленных систем управления и исходных кодов вредоносных программ.

Стандарты ANSI/ISA99, которые обеспечивают кибербезопасность систем автоматизации и управления, обеспечивают хорошую основу для разработки политики безопасности, ориентированной на промышленные системы. Эти стандарты представляют собой общую концепцию кибербезопасности, а также модели и отдельные элементы системы безопасности и являются важными документами для стандарта IEC 62443 «Безопасность систем управления».

В стандарте IEC 62443 описаны методы повышения безопасности в промышленных сетях, охватывающие всю область промышленной безопасности без отраслевых ограничений (Вихляев, 2020). Промышленные брандмауэры, разработанные в соответствии с этим стандартом, уже представлены на рынке, которые позволяют создавать безопасные зоны с помощью ПЛК и OPC-серверов.

В некоторых отраслях промышленности существуют свои собственные специфические стандарты сетевой безопасности. Например, стандарт NERC CIP разработан для энергетики Северной Америки. В отличие от стандарта IEC 62443, сертификация NERC CIP является обязательной в США, в то время как для стандарта

IEC 62443 — это добровольный процесс.

Современный рынок промышленной автоматизации открывает большие возможности, но его рост значительно замедляется из-за экономических и политических факторов. Очевидно, что автоматизация является главным двигателем прогресса и должна продолжать развиваться (Воронцов, 2019).

Промышленная автоматизация обеспечивает высокое качество продукции, снижает финансовые затраты, увеличивает конкурентоспособность многих товаров и улучшает безопасность на производстве для сотрудников.

Этапы производства различных продуктов имеют свои особенности, такие как:

- сложность выполнения отдельных процессов;
- высокая чувствительность к сбоям и отклонениям в определенных режимах;
- присутствие вредных летучих веществ в производственной зоне.

Эти факторы подчеркивают необходимость применения современных технологий автоматизации как важной меры безопасности.

Следует отметить, что все системы управления на промышленных предприятиях основаны на программных комплексах, которые учитывают особенности производственных процессов. Поскольку производственные предприятия относятся к объектам повышенной безопасности, для повышения надежности систем внедряются резервные копии файлов и данных автоматизации. Системы автоматического управления создаются по модульному принципу, что позволяет быстро заменять неисправные элементы и восстанавливать их функции.

Сегодня целесообразность автоматизации должна быть продемонстрирована на примере успешных проектов с использованием цифровых данных, которые показывают важность приложения для конкретного бизнеса (Иванов, 2021). Важно донести до целевой аудитории, что автоматизация промышленного предприятия обходится не так дорого, как установка турбины или строительство нового цеха.

Создание защищенной технологической сети основано на принципе глубокой защиты. Это означает, что защита сети передачи данных не ограничивается только периметром, но и включает в себя фрагментацию сети с выделением критических областей в безопасные зоны. Каждая зона должна быть защищена отдельным промышленным брандмауэром, который обеспечит высокий уровень безопасности и поддержит необходимые коммуникации. Промышленные брандмауэры оптимизированы для работы с протоколами Modbus и OPC, а их усовершенствование позволяет ограничить доступ к критически важным сегментам сети.

Помимо технических решений в области кибербезопасности, важно уделять внимание организационным аспектам, в частности обучению персонала. Сотрудники должны быть знакомы с правилами и средствами обеспечения информационной безопасности, а также с разработанными политиками и стандартами. Поскольку специалисты по автоматизированным системам часто обладают ограниченными знаниями в области кибербезопасности, важно объяснить им важность этого вопроса и ввести обязательную программу обучения бизнесу (Камаев и др., 2019). Различные категории сотрудников, такие как посетители, подрядчики, операторы, инженеры, обслуживающий персонал и менеджеры, должны быть осведомлены о своих ролях и обя-занностях, а также получать информацию о разрешенных и запрещенных действиях.

В производственной зоне технический персонал должен уметь обращаться с охранным оборудованием, менеджеры должны знать алгоритмы действий в случае возникновения угроз безопасности автоматизированных систем управления.

В настоящее время основной проблемой кибербезопасности промышленных предприятий является непонимание специалистами автоматизированных систем управления важности применения соответствующих инструментов, даже при наличии необходимых технологий. Владельцы критически важных объектов часто недооценивают информационные угрозы по целому ряду причин. Наблюдается заметная нехватка необходимых процедур, таких как проверка информации, тестирование на проникновение, сканирование уязвимостей и обучение персонала (Кирсанов, 2021). На сегодняшний день не установлено никаких обязательных стандартов промышленной кибербезопасности.

Также не существует единой, понятной методологии, в рамках которой эксперты по информационной безопасности могли бы рекомендовать меры по достижению адекватного уровня защиты автоматизированных систем управления.

Кроме того, на ситуацию негативно влияет сложный бюрократический процесс внесения изменений в работу ответственных технологических центров. Строгие внутренние правила компании не допускают внесения изменений в уже сертифицированные системы, даже если речь идет об обновлениях операционной системы. При приемке систем методы тестирования программного обеспечения часто не предполагают проверки встроенных функций информационной безопасности (Клепиков и др., 2019). К сожалению, уровень безопасности в основном обеспечивается только за счет ограничения доступа пользователей с помощью пароля, который часто хранится в виде обычного текста в базе данных приложения или на листке бумаги, приклеенном к экрану.

Если говорить о вычислительном оборудовании, используемом в автоматизированных системах управления технологическими процессами, то оно обычно начинает свою работу с устаревшего внутреннего исполняемого кода. Несмотря на наличие на сайте производителя обновленной прошивки, которая может устранить известные проблемы с информационной безопасностью, никто не проверяет ее доступность даже на этапе разработки системы, поскольку это не является приоритетом.

Также стоит учитывать, что автоматизация технологических процессов часто осуществляется сторонними подрядчиками, которые в основном сосредоточены на операционных аспектах проекта, поскольку за это они получают оплату (Клюев и др., 2019). В этом контексте внедрение эффективных мер информационной безопасности можно рассматривать как ненужные затраты. Поэтому заказчикам необходимо осознавать важность кибербезопасности, формулировать соответствующие требования к подрядчикам и контролировать их выполнение.

Промышленная автоматизация — это совокупность методов и технологий, а также программного обеспечения, используемых для создания автоматизированных систем управления и технологических процессов производства без необходимости непосредственного участия оператора.

Автоматизация производственных процессов помогает улучшить качество продукции, снизить затраты и повысить конкурентоспособность.

Использование автоматизированных систем управления технологическими

процессами снижает затраты на содержание менее квалифицированного персонала, что, в свою очередь, повышает долговечность оборудования и надежность машин.

Современная промышленная автоматизация также способствует экономии материалов, сырья и ресурсов, а также повышает безопасность производственных процессов и условия труда сотрудников (Кондаков и др., 2021). Внедрение современных автоматизированных компонентов позволяет достичь следующих результатов:

1. снижение простоя оборудования на 10–15 %;
2. сокращение потребления электрической энергии и других энергоресурсов до 35 %;
3. уменьшение затрат на обслуживание производства до 30 %;
4. снижение объемов бракованной продукции.

Учитывая текущее экономическое положение, эти аспекты становятся особенно важными.

Автоматизированная система включает в себя ряд компонентов, обеспечивающих управление объектами и сбор информации о текущих процессах на предприятии (Пищик, 2020). Основные компоненты промышленной автоматизации и их классификация включают:

1. устройства для защиты от импульсного перенапряжения в силовых и информационных линиях;
2. блоки питания, размещаемые в шкафах управления;
3. промышленные сетевые коммутаторы, выполненные в прочных защитных корпусах, что делает их подходящими для промышленного применения;
4. устройства, включающие интерфейсные реле для измерений и контроля;
5. модули ввода и вывода, которые объединяют системы сбора данных и полностью соответствуют требованиям решаемых задач, совместимы с любыми PLS и IPC системами.

Благодаря использованию новых компонентов автоматизация промышленных установок становится более понятной и прозрачной, так как осуществляется контроль и управление через единую информационную базу, к которой подключены все отделы (Попова и др., 2019).

Таким образом, промышленно-технологическая автоматизация предлагает множество преимуществ, таких как:

1. ведение оперативного учета производства;
2. управление затратами и своевременное принятие управленческих решений;
3. планирование работы и распределение трудовых ресурсов и мощностей;
4. оперативное управление производственным циклом;
5. формирование производственной отчетности;
6. комплексный анализ и мониторинг деятельности предприятия;
7. расчет себестоимости производимых товаров.

Важно отметить, что большинство систем промышленной автоматизации организованы по трехуровневой модели:

1. На первом уровне находятся системы контроля и автоматического регулирования технологических подсистем и объектов, основанные на микропроцессорных контроллерах, а также оборудовании КИПиА, измерителях и счетчиках.

2. Второй уровень включает компоненты для концентрации, обработки и передачи информации между нижним и верхним уровнями.

3. Верхний уровень состоит из устройств для передачи, хранения, накопления и предоставления информационных файлов, включая средства локальной вычислительной сети, которая связывает рабочие подсистемы.

Автоматизация промышленных объектов позволяет получить полностью механизированные ключевые производственные и управленческие бизнес-процессы.

Что в свою очередь значительно уменьшает рутину и повышает производительность труда рабочих на производстве, а само предприятие становится конкурентоспособным, увеличивая тем самым на рынке свою себестоимость.

Сети промышленной автоматизации и управления — это сложные системы, состоящие из аппаратных и программных компонентов, которые обеспечивают управление технологическими процессами на предприятиях (Селевцов, 2019). Эти сети обладают уникальными особенностями, отличающими их от обычных корпоративных сетей, которые требуют особых подходов к обеспечению безопасности. Давайте рассмотрим основные возможности промышленной автоматизации и сетей управления более подробно:

Программируемые логические контроллеры (PLC), используются для автоматизации задач управления и мониторинга технологических процессов. PLC выполняют функции сбора данных, обработки сигналов и управления исполнительными механизмами. Распределённые управляющие системы (DCS), применяются для управления сложными процессами на крупных предприятиях, таких как нефтехимические заводы. DCS обычно включают в себя несколько уровней контроля и взаимодействуют с различными процессами (Снытников, 2020). Системы управления на основе SCADA, предоставляют мониторинг и управление в реальном времени, собирая данные от различных датчиков и контроллеров и представляя их в удобной форме для операторов. Исполнительные механизмы, включают в себя насосы, клапаны, двигатели и другие устройства, которые выполняют физическое воздействие на технологический процесс. Датчики и измерительные приборы, служат для сбора данных о состоянии технологического процесса, таких как температура, давление, уровень и другие параметры. Коммуникационные устройства и протоколы: коммутаторы и маршрутизаторы: обеспечивают связь между различными компонентами сети и передачу данных между контроллерами, датчиками и исполнительными механизмами. Протоколы связи, включают в себя специализированные промышленные протоколы, такие как Modbus, Profibus, Ethernet/IP, OPC, которые предназначены для обмена данными между компонентами ПСАУ и имеют особенности в области надежности и реального времени (Стрельцов, 2019).

Промышленные сети автоматизации и управления должны обеспечивать работу в реальном времени, что означает необходимость немедленного отклика на изменения в процессе и поддержания бесперебойного контроля. Это требует высокой надежности и низкой задержки передачи данных.

Промышленные сети автоматизации и управления должны быть высоко отказоустойчивыми, обеспечивать непрерывную работу даже в случае сбоя отдельных компонентов. Это достигается за счет резервирования критических компонентов и реализации механизмов аварийного восстановления.

Промышленные сети автоматизации и управления часто интегрируются с

другими системами, такими как корпоративные ИТ-системы, облачные платформы и системы бизнес-аналитики. Это требует возможности масштабирования и интеграции с различными технологическими решениями (Хорев, 2019).

Промышленные сети автоматизации и управления требуют строгого контроля доступа, чтобы предотвратить несанкционированное вмешательство. Это включает в себя аутентификацию и авторизацию пользователей, а также управление доступом к критическим компонентам системы.

Для обеспечения безопасности данных и предотвращения утечек используется шифрование данных и защитные механизмы для коммуникационных каналов (Чернобровцев, 2019). Это важно для защиты от перехвата данных и их модификации.

Промышленные сети автоматизации управления должны иметь системы мониторинга и управления событиями для своевременного обнаружения и реагирования на инциденты безопасности. Это включает в себя использование систем обнаружения вторжений (IDS), систем управления событиями безопасности (SIEM) и других инструментов.

Промышленные сети играют ключевую роль в автоматизации и управлении производственными процессами. Эти сети обеспечивают связь между различными устройствами, такими как контроллеры, датчики и системы управления, позволяя эффективно обмениваться данными и координировать действия в реальном времени. Важно понимать их характеристики, компоненты и протоколы, используемые в промышленной среде. Ниже представлена таблица, которая обобщает основные аспекты промышленных сетей, включая их типы, устройства, протоколы связи и меры безопасности. Информация, представленная в таблице 1 поможет глубже понять структуру и функциональность промышленных сетей.

Таблица 1. Промышленные сети и характеристика их компонентов

Компонент или характеристика	Описание	Примеры
Тип сети	Сети, используемые для управления промышленными процессами.	Ethernet, Profibus, Modbus.
Устройства	Основные устройства, подключенные к сети.	PLC, SCADA-системы, датчики.
Протоколы связи	Протоколы, используемые для передачи данных.	TCP/IP, MQTT, OPC UA.
Типология сети	Структура, в которой организованы соединения.	Звезда, шина, кольцо.
Безопасность сети	Меры, принимаемые для защиты сети от угроз.	Системы IDS/IPS, шифрование данных.
Управление доступом	Механизмы контроля доступа к сети.	Аутентификация по ролям, VPN.
Мониторинг сети	Инструменты для контроля состояния сети.	SNMP, NetFlow.

Резервирование	Методы обеспечения непрерывности работы сети.	Дублирование оборудования, горячие резервуары.
Интеграция с IT-системами	Связь между промышленными и информационными системами.	Использование API, шлюзов.
Поддержка стандартов	Соответствие отраслевым стандартам и нормативам.	ISA/IEC 62443, ISO 27001.

Безопасность промышленных сетей является важным аспектом, учитывающим угрозы и уязвимости, которые могут повлиять на стабильность и безопасность производственных процессов. Механизмы управления доступом и мониторинга состояния сети помогают защитить системы от несанкционированного доступа и атак.

Кроме того, поддержка отраслевых стандартов, таких как ISA/IEC 62443 и ISO 27001, способствует созданию надежных и безопасных инфраструктур, что является необходимым условием для успешной работы в условиях современного производства.

Важным аспектом является защита физического доступа к критическим компонентам промышленных сетей автоматизации и управления. Это может включать в себя контроль доступа в серверные помещения, использование видеонаблюдения и системы сигнализации.

Развитие технологий IoT и Industry 4.0:

Внедрение технологий Интернета вещей (IoT) и концепций Industry 4.0 изменяет структуру промышленных систем автоматизации и управления добавляя новые устройства и узлы. Это требует дополнительных мер безопасности и новых подходов к защите.

Увеличение числа кибератак и уязвимостей в системах управления требует постоянного обновления и адаптации методов защиты (Шишов, 2021). Новые виды угроз, такие как атаки на промышленные интернет-протоколы, требуют особого внимания.

Для систематизации подходов к обеспечению безопасности промышленных сетей автоматизации и управления, в таблице 2 представлены ключевые методы и технологии, применяемые для защиты промышленных сетей. Таблица 2 охватывает различные аспекты безопасности, включая управление доступом, сетевые и коммуникационные меры, программные и аппаратные средства, а также организационные меры. Каждая категория включает в себя конкретные методы, их цели и примеры применения.

Таблица 2. Методы обеспечения безопасности промышленных сетей автоматизации и управления

Категория	Метод/Технология	Описание	Цели	Примеры
1. Управление доступом	Аутентификация и авторизация	Процедуры для проверки идентичности пользователей и их прав доступа.	Процедуры для проверки идентичности пользователей и их прав доступа.	Использование двухфакторной аутентификации ролевого контроля доступа.
	Управление правами доступа	Определение и управление правами доступа пользователей и групп.	Гарантия, что только авторизованные пользователи имеют доступ к критическим системам.	Системы контроля доступа (IAM), управление правами.
2.Сетевые и коммуникационные меры	Сегментация сети	Разделение сети на логические сегменты для ограничения распространения угроз.	Локализация и минимизация воздействия атак.	Виртуальные локальные сети (VLAN), межсетевые экраны (firewalls).
	Шифрование данных	Использование криптографических методов для защиты данных при передаче и хранении.	Защита данных от перехвата и несанкционированного доступа.	Протоколы SSL/ TLS, шифрование в облаке.
	Мониторинг и управление трафиком	Слежение за сетевым трафиком и выявление аномалий, потенциальных угроз.	Обнаружение и предотвращение атак в реальном времени.	Системы управления событиями безопасности (SIEM), IDS/IPS.
3.Программные и аппаратные меры	Антивирусные и антивредоносные программы	антивредоносные программы ПО для обнаружения, удаления и предотвращения вредоносного ПО.	Защита от вирусов, червей и других вредоносных программ.	Антивирусные решения, системы обнаружения вредоносных программ.
	Патчи и обновления	Регулярное обновление программного обеспечения для устранения известных уязвимостей.	Устранение уязвимостей и улучшение безопасности.	Автоматическое обновление ПО, управление патчами.
	Физическая безопасность	Меры по защите оборудования и инфраструктуры от физического доступа.	Защита от физического вмешательства и кражи.	Контроль доступа в серверные комнаты, видеонаблюдение.
4.Организационные методы	Политики и процедуры безопасности	Разработка и внедрение внутренних политик и процедур для обеспечения безопасности.	Стандартизация и упрощение процессов обеспечения безопасности.	Политики безопасности, процедуры инцидент-менеджмента.
	Обучение и повышение осведомленности	Обучение сотрудников принципам кибербезопасности и методам предотвращения угроз.	Снижение риска ошибок человеческого фактора.	Программы обучения по безопасности, тренинги по реагированию на инциденты.
5.Инструменты и технологии	Системы обнаружения и предотвращения вторжений (IDS/IPS)	Системы для обнаружения и предотвращения попыток несанкционированного доступа и атак.	Реагирование на угрозы и предотвращение атак.	Внедрение IDS/IPS в сети предприятия.

	Системы управления событиями безопасности (SIEM)	Инструменты для сбора, анализа и корреляции данных безопасности из различных источников.	Обеспечение централизованного управления и анализа безопасности.	Решения SIEM, такие как Splunk, ArcSight.

Итак, в таблице показан контроль доступа, который включает в себя меры аутентификации и авторизации, управление правами доступа, которые необходимы для обеспечения того, чтобы только авторизованные пользователи могли получить доступ к критически важным системам и данным. Сетевые и коммуникационные меры, охватывающие такие технологии и приемчики, как сегментация сети, шифрование данных и мониторинг трафика, направленные на защиту данных во время передачи и предотвращение несанкционированного доступа. Программные и аппаратные меры включают использование антивирусных решений, регулярные обновления программного обеспечения, а также меры по обеспечению безопасности физического оборудования, которые помогают защититься от вредоносных программ и физического вмешательства (Язов, 2019). Организационные меры указывают на важность разработки и внедрения политики в области безопасности, а также обучения сотрудников, что способствует установлению стандартов безопасности и повышению осведомленности сотрудников. Инструменты и технологии, использование специализированных систем обнаружения и предотвращения вторжений, а также управление инцидентами безопасности, что обеспечивает эффективное реагирование на угрозы и инциденты.

Эта таблица предназначена для того, чтобы дать исчерпывающий обзор методов обеспечения безопасности для промышленной автоматизации и сетей управления, которые могут быть адаптированы и внедрены в соответствии со спецификой и потребностями конкретного предприятия. Включение различных категорий методов и технологий в таблицу позволяет в полной мере понять подходы к защите промышленных сетей и способствует созданию эффективной системы безопасности.

Обеспечение безопасности промышленных сетей автоматизации и управления на предприятиях представляет собой комплексную задачу, требующую интеграции различных аспектов — технических, организационных и человеческих. Важно применять современные технологии, такие как шифрование и системы обнаружения вторжений, а также уделять внимание обучению персонала.

Выводы

Адаптация к постоянно меняющемуся ландшафту угроз является ключевым элементом защиты, что подразумевает регулярную оценку рисков и обновление мер безопасности в соответствии с новыми вызовами. Учет существующих стандартов и рекомендаций, таких как ISA/IEC 62443, помогает выработать эффективные политики безопасности и минимизировать риски.

С учетом растущего взаимодействия информационных и операционных технологий необходимо разрабатывать методы, которые обеспечат совместную безопасность этих систем, учитывая их уникальные характеристики. Эффективные системы мониторинга и быстрого реагирования на инциденты играют критически важную роль в минимизации последствий потенциальных атак, что требует наличия четких протоколов действий.

Безопасность должна стать приоритетом на всех уровнях организации — от руководства до операционного персонала. Создание культуры безопасности, где все

сотрудники вовлечены в процессы защиты, способствует снижению рисков. Важно также активно исследовать и внедрять новые технологии, такие как искусственный интеллект и машинное обучение, чтобы повысить уровень автоматизации и эффективности защиты промышленных сетей. Таким образом, безопасность промышленных сетей требует постоянного совершенствования методов и стратегий, а также взаимодействия всех заинтересованных сторон для обеспечения надежной защиты.

ЛИТЕРАТУРА

Афонин А.М., Царегородцев Ю.Н., Петрова А.М. (209). Теоретические основы разработки и моделирования систем автоматизации: Учебное пособие. — М.: Форум. — 336 с.

Баранова Е.К., Бабаш А.В. (2020). Информационная безопасность и защита информации: учебное пособие. 3-е изд. перераб. и доп. — М.: РИОР; ИНФРА-М. — 322 с.

Бирюков А.А. (2020). Информационная безопасность: защита и нападение. 2-е изд. перераб. и доп. — М.: ДМК Пресс. — 434 с.

Вихляев А.А. (2020). К вопросу совершенствования методов обработки, хранения, анализа и систематизации больших данных на современном этапе. — В: Государственное управление и развитие: глобальные угрозы и структурные изменения: Сб. ст. междунар. конф. сессий. — С. 137–141.

Воронцов А.А. (2019). Автоматизированные системы управления технологическими процессами. Вопросы безопасности. Jetlnfo. — № 5. — С. 89–96.

Иванов А.А. (2021). Автоматизация технологических процессов и производств: Учебное пособие. — М.: Форум. — 224 с.

Камаев В.А., Лежебоков В.В. (2019). Разработка и применение модели автоматизированной системы управления информационными процессами к задаче мониторинга состояния оборудования. Вестник компьютерных и информационных технологий. — № 9. — 18–22.

Кирсанов С.В. (2021). Метод оценки угроз информационной безопасности АСУ ТП газовой отрасли. — Доклады ТУСУР. — № 2(28). — 112–115.

Клепиков В.В., Схиртладзе А.Г., Султан-заде Н.М. (2019). Автоматизация производственных процессов: Учебное пособие. — М.: Инфра-М. — 351 с.

Клюев А.С., Ротач В.Я., Кузищин В.Ф. (2019). Автоматизация настройки систем управления. — М.: Альянс. — 272 с.

Кондаков В.В., Краснобородько А.А. (2021). Информационная безопасность систем физической защиты: Учебное пособие. — М.: МИФИ. — 48 с.

Пищик Б.Н. (2020). Безопасность АСУ ТП. Вычислительные технологии. — Спецвыпуск. — Т. 18. — 170–175.

Попова А.Д., Богданов П.А., Быков Д.В. (2019). Разработка автоматизированной системы моделирования угроз безопасности. Студенческий: электрон. научн. Журн. — № 7(27). URL: https://sibac.info/journal/student/27/103048

Селевцов Л.И. (2019). Автоматизация технологических процессов: Учебник. — М.: Academia. — 160 с. Снытников А.А. (2020). Лицензирование и сертификация в области защиты информации. —М.: Гелиос АРВ. — 192 с.

Стрельцов А.А. (2019). Правовое обеспечение информационной безопасности: теоретические и методологические основы. — Минск. — 304 с.

Хорев А.А. (2019). Защита информации от утечки по техническим каналам: Учебное пособие. — М.: МО РФ. — 350 с.

Чернобровцев А. (2019). Защита АСУ ТП. Computerworld Россия. — № 10. — 25–32.

Шишов О.В. (2021). Современные технологии промышленной автоматизации: учебное пособие. — Саранск: Изд-во Мордов. ун-та. — 276 с.

Язов Ю.К. (2019). Основы методологии количественной оценки эффективности защиты информации в компьютерных сетях. — Ростов-на-Дону: Издательство СКНЦ ВШ. — 220 с.

REFERENCES

Afonin, A.M., Caregorodcev, Ju.N., Petrova, A.M. (2019). Teoreticheskie osnovy razrabotki i modelirovanija sistem avtomatizacii: Uchebnoe posobie [Theoretical foundations of the development and modeling of automation

systems: A textbook]. —Moscow: Forum. — 336 p. [In Russ.].

Baranova E.K., Babash A.V. (2020). Informacionnaja bezopasnost' i zashhita informacii: ucheb. posobie [Information security and data protection: A textbook]. 3rd ed. — Moscow: RIOR; INFRA-M. — 322 p. [In Russ.].

Birjukov A.A. (2020). Informacionnaja bezopasnost': zashhita i napadenie [Information security: Defense and attack]. 2nd ed. — Moscow: DMK Press. — 434 p. [In Russ.].

Vihljaev A.A. (2020). K voprosu sovershenstvovanija metodov obrabotki, hranenija, analiza i sistematizacii bol'shih dannyh na sovremennom jetape [On the improvement of methods for processing, storage, analysis, and systematization of big data at the current stage]. In: Gosudarstvennoe upravlenie i razvitie: global'nye ugrozy i strukturnye izmenenija: Sbornik statej mezhdunarodnoj konferencii [State Governance and Development: Global Threats and Structural Changes: Proceedings of the International Conference]. — Pp. 137–141. [In Russ.].

Voroncov A.A. (2019). Avtomatizirovannye sistemy upravlenija tehnologicheskimi processami. Voprosy bezopasnosti [Automated control systems for technological processes. Security issues]. — Jetlnfo. — 5. — 89–96. [In Russ.].

Ivanov A.A. (2021). Avtomatizacija tehnologicheskih processov i proizvodstv: — Uchebnoe posobie [Automation of technological processes and productions: A textbook]. — Moscow: Forum. — 224 p. [In Russ.].

Kamaev V.A., Lezhebokov V.V. (2019). Razrabotka i primenenie modeli avtomatizirovannoj sistemy upravlenija informacionnymi processami k zadache monitoringa sostojanija oborudovanija [Development and application of an automated system management model for monitoring equipment condition]. Vestnik komp'juternyh i informacionnyh tehnologij [Bulletin of Computer and Information Technologies]. — 9. — 18–22. [In Russ.].

Kirsanov S.V. (2021). Metod ocenki ugroz informacionnoj bezopasnosti ASU TP gazovoj otrasli [Method for assessing information security threats of the industrial control system in the gas industry]. — Doklady TUSUR. — 2(28). — 112–115. [In Russ.].

Klepikov V.V., Shirtladze A.G., Sultan-zade N.M. (2019). Avtomatizacija proizvodstvennyh processov: Uchebnoe posobie [Automation of production processes: A textbook]. — Moscow: Infra-M. — 351 p. [In Russ.].

Kljuev A.S., Rotach V.Ja., Kuzishhin V.F. (2019). Avtomatizacija nastrojki sistem upravlenija [Automation of control system settings]. — Moscow: Al'jans. — 272 p. [In Russ.].

Kondakov V.V., Krasnoborod'ko A.A. (2021). Informacionnaja bezopasnost' sistem fizicheskoj zashhity: uchebnoe posobie [Information security of physical protection systems: A textbook]. — Moscow: MIFI. — 48 p. [In Russ.].

Pishhik B.N. (2020). Bezopasnost' ASU TP [Safety of industrial control systems]. Vychislitel'nye tehnologii [Computational Technologies]. — Special Issue. — 18. — 170–175. [In Russ.].

Popova A.D., Bogdanov P.A., Bykov D.V. (2019). Razrabotka avtomatizirovannoj sistemy modelirovanija ugroz bezopasnosti [Development of an automated system for modeling security threats]. Studencheskij: jelektronnyj nauchnyj zhurnal [Student: Electronic Scientific Journal]. — 7(27). Available at: https://sibac.info/journal/student/27/103048 [In Russ.].

Selevcov L.I. (2019). Avtomatizacija tehnologicheskih processov: Uchebnik [Automation of technological processes: A textbook]. — Moscow: Academia. — 160 p. [In Russ.].

Snytnikov A.A. (2020). Licenzirovanie i sertifikacija v oblasti zashhity informacii [Licensing and certification in the field of information protection]. — Moscow: Gelios ARV. — 192 p. [In Russ.].

Strel'cov A.A. (2019). Pravovoe obespechenie informacionnoj bezopasnosti: teoreticheskie i metodologicheskie osnovy [Legal provision of information security: Theoretical and methodological foundations]. — Minsk. — 304 p. [In Russ.].

Horev A.A. (2019). Zashhita informacii ot utechki po tehnicheskim kanalam: Uchebnoe posobie [Information leakage protection through technical channels: A textbook]. — Moscow: MO RF. — 350 p. [In Russ.].

Chernobrovcev A. (2019). Zashhita ASU TP [Protection of industrial control systems]. Computerworld Rossija [Computerworld Russia]. — 10. — 25–32. [In Russ.].

Shishov O.V. (2021). Sovremennye tehnologii promyshlennoj avtomatizacii: uchebnoe posobie [Modern technologies of industrial automation: A textbook]. — Saransk: Mordov. un-ta. — 276 p. [In Russ.].

Jazov Ju.K. (2019). Osnovy metodologii kolichestvennoj ocenki jeffektivnosti zashhity informacii v komp'juternyh setjah [Fundamentals of methodology for quantitative assessment of information security efficiency in computer networks]. — Rostov-na-Donu: Izdatel'stvo SKNC VSh. — 220 p. [In Russ.].

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Правила оформления статьи для публикации в журнале на сайте:
https://journal.iitu.edu.kz
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Собственник: АО «Международный университет информационных технологий» (Казахстан, Алматы)

ОТВЕТСТВЕННЫЙ РЕДАКТОР
Мрзабаева Раушан Жалиқызы

КОМПЬЮТЕРНАЯ ВЕРСТКА
Асанова Жадыра

Подписано в печать 14.09.2024.
Формат 60x881/8. Бумага офсетная. Печать - ризограф. 9,0 п.л. Тираж 100
050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09).

Издание Международного университета информационных технологий
Издательский центр КБТУ, Алматы, ул. Толе би, 59