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

Г.Т. Алин
БАҒДАРЛАМАЛЫҚ ҚҰРАМДЫ ЖАСАУ ЖОБАСЫН БАСҚАРУ: ЖОБАДА МЕТРИКА ЖӘНЕ САПА БАСҚАРУ.....8
Ж. Досбаев, Л. Илипбаева, А. Сулиман
ОҚИҒАЛАРДЫ АУДИОСИГНАЛДАР НЕГІЗІНДЕ ТЕРЕҢ ОҚЫТУ ӘДІСТЕРІ НЕГІЗІНДЕ АНЫҚТАУ.....23
А.Б. Ембердіева, I.C. Young, С.Е. Маманова, С.Б. Муханов
ЖАСАНДЫ НЕЙРОНДЫҚ ЖЕЛІЛЕРДІ ҚҰРУ ҮШІН КЕРІ ТАРАЛУ ӘДІСІНІҢ МАТЕМАТИКАЛЫҚ ТӘСІЛІ.....32
Р. Лисневский, М. Гладка, С. Билощицкая
IOT ШЕШІМДЕРІН ҚОЛДАНА ОТЫРЫП, ЖЕЛІДЕГІ ЭНЕРГИЯ ШЫҒЫНЫН ТАЛДАУ.....49
А. Мырзакерімова, А. Хикметов
МЕДИЦИНАДАҒЫ МАТЕМАТИКАЛЫҚ МОДЕЛЬДЕР: ДИАГНОСТИКА ПРОЦЕСІН АВТОМАТТАНУДАҒЫ ЗАМАНАУ ТӘСІЛДЕР.....60
А.Б. Нургалыков, А.М. Әкім
ANDROID ЖҮЙЕСІНДЕ КОРУТИНДЕРДІ ҚОЛДАНУ АРҚЫЛЫ КӨПТАПСЫРМАЛЫЛЫҚТЫ ОҢТАЙЛАНДЫРУ: ӨНІМДІЛІКТІ САЛЫСТЫРМАЛЫ ТАЛДАУ.....71
Ю. Сокыран, Т. Бабенко, И. Пархоменко, Л. Мирутенко
OSINT ЗЕРТТЕУЛЕРІН ЖҮРГІЗУДІҢ КОМПЬЮТЕРЛІК КӨРУ ӘДІСТЕРІ..80
Д. Утебаева, Л. Илипбаева
БАҒДАРЛАМАМЕН АНЫҚТАЛАТЫН РАДИО-ЖҮЙЕНІҢ (SDR) ЖӘНЕ ИНТЕЛЛЕКТУАЛДЫ АКУСТИКАЛЫҚ СЕНСОРДЫҢ ОРЫНДАУ ҚАБІЛЕТТЕРІН ҰШҚЫШСЫЗ ҰШУ АППАРАТТАРЫН ТАНУҒА САЛЫСТЫРМАЛЫ ЗЕРТТЕУ.....90

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАРҒА АРНАЛҒАН

Н.Т. Дузбаев, А. Макеев, Е.Е. Оспанов
КӘСІПОРЫНДАРДАҒЫ ӨНДІРІСТІК АВТОМАТТАНДЫРУ ЖӘНЕ БАСҚАРУ ЖЕЛІЛЕРІНІҢ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІН ӘЗІРЛЕУ.....99
А. Макеев
ӨНЕРКӘСІПТІК КӘСІПОРЫНДАРДЫ ҚОРҒАУДЫҢ АВТОМАТТАНДЫРЫЛҒАН ЖҮЙЕСІ.....115

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Г.Т. Алин
УПРАВЛЕНИЕ ПРОЕКТАМИ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ: УПРАВЛЕНИЕ КОНФИГУРАЦИЯМИ, КОНТРОЛЬ ВЕРСИЙ И РЕЛИЗОВ ПРОГРАММНОГО ПРОДУКТА.....8
Ж. Досбаев, Л. Илипбаева, А. Сулиман
ОБНАРУЖЕНИЕ СОБЫТИЙ НА ОСНОВЕ АУДИОСИГНАЛОВ С ПРИМЕНЕНИЕМ ГЛУБОКОГО ОБУЧЕНИЯ.....23
А.Б. Ембердиева, I.C. Young, С.Е. Маманова, С.Б. Муханов
МАТЕМАТИЧЕСКИЙ ПОДХОД МЕТОДА ОБРАТНОГО РАСПРОСТРАНЕНИЯ ДЛЯ ПОСТРОЕНИЯ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ.....32
Р. Лисневский, М. Гладка, С. Билощицкая
АНАЛИЗ ЭНЕРГОПОТРЕБЛЕНИЯ В СЕТИ С ИСПОЛЬЗОВАНИЕМ IOT-РЕШЕНИЙ.....49
А. Мырзакерімова, А. Хикметов
МАТЕМАТИЧЕСКИЕ МОДЕЛИ В МЕДИЦИНЕ: СОВРЕМЕННЫЕ ПОДХОДЫ К АВТОМАТИЗАЦИИ ДИАГНОСТИЧЕСКОГО ПРОЦЕССА.....60
А.Б. Нургалыков, А.М. Аким
ОПТИМИЗАЦИЯ МНОГОЗАДАЧНОСТИ В ANDROID С ПОМОЩЬЮ КОРУТИН: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОИЗВОДИТЕЛЬНОСТИ.....71
Ю. Сокиран, Т. Бабенко, И. Пархоменко, Л. Мирутенко
МЕТОДЫ КОМПЬЮТЕРНОГО ЗРЕНИЯ ДЛЯ ПРОВЕДЕНИЯ OSINT-ИССЛЕДОВАНИЙ.....80
Д. Утебаева, Л. Илипбаева
СРАВНИТЕЛЬНОЕ ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК ПРОГРАММНО-КОНФИГУРИРУЕМОЙ РАДИОСИСТЕМЫ (SDR) И ИНТЕЛЛЕКТУАЛЬНЫХ АКУСТИЧЕСКИХ ДАТЧИКОВ ДЛЯ ОБНАРУЖЕНИЯ БПЛА.....90

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Н.Т. Дузбаев, А. Макеев, Е.Е. Оспанов
РАЗРАБОТКА МЕТОДОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ СЕТЕЙ АВТОМАТИЗАЦИИ И УПРАВЛЕНИЯ НА ПРЕДПРИЯТИЯХ.....99
А. Макеев
АВТОМАТИЗИРОВАННАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ.....115

INFORMATION TECHNOLOGY

G.T. Alin
SOFTWARE DEVELOPMENT PROJECT MANAGEMENT: METRICS AND QUALITY MANAGEMENT IN PROJECTS.....8
Zh. Dosbayev, L. Ilipbayeva, A. Suliman
AUDIOSIGNAL BASED EVENT DETECTION USING DEEP LEARNING TECHNIQUES.....23
A.B. Yemberdiyeva, I.C. Young, S.Ye. Mamanova, S.B. Mukhanov
MATHEMATICAL APPROACH OF THE BACKPROPAGATION METHOD FOR CONSTRUCTING ARTIFICIAL NEURAL NETWORKS.....32
R. Lisnevskyi, M. Gladka, S. Biloshchytska
ANALYSIS OF ENERGY COSUMPTION IN THE NETWORK USING IOT SOLUTIONS.....49
A. Myrzakerimova, A.K. Khikmetov
MATHEMATICAL MODELS IN MEDICINE: MODERN APPROACHES TO DIAGNOSTIC PROCESS AUTOMATION 60
A.B. Nurgalykov, A.M. Akim
OPTIMIZATION OF MULTITASKING IN ANDROID USING COROUTINES: A COMPARATIVE PERFORMANCE ANALYSIS.....71
Y. Sokyran, T. Babenko, I. Parkhomenko, L. Myrutenko
COMPUTER VISION METHODS FOR CONDUCTING OSINT INVESTIGATIONS.....80
D. Utebayeva, L. Ilipbayeva
A COMPARATIVE STUDY OF SOFTWARE-DEFINED RADIO (SDR) AND SMART ACOUSTIC SENSOR PERFORMANCE FOR UAV DETECTION.....90

INFORMATION SECURITY AND COMMUNICATION TECHNOLOGIES

N.T. Duzbayev, A. Makeyev, Y.Y. Ospanov
DEVELOPMENT OF METHODS FOR ENSURING THE SECURITY OF INDUSTRIAL AUTOMATION AND CONTROL NETWORKS AT ENTERPRISES.....99
A. Makeyev
AUTOMATED SECURITY SYSTEM FOR INDUSTRIAL ENTERPRISES.....115

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 5. Is. 3. Number 19 (2024). Pp. 115–127
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2024.19.3.010

AUTOMATED SECURITY SYSTEM FOR INDUSTRIAL ENTERPRISES

A. Makeyev
LLC "Terralink Technologies", Almaty, Kazakhstan.
E-mail: alibekmakeyev@gmail.com

Alibek Makeyev — analyst, LLC "Terralink Technologies", Almaty, Kazakhstan
E-mail: alibek-makeyev@gmail.com, https://orcid.org/0009-0001-5174-825X.

Abstract. Security systems have become an integral part of the existence of modern industrial enterprises. For such a system to function smoothly, it is necessary to create better conditions and automate this process. Trends in the development of modern security systems are directly related to extensive automation and integration, which affect not only security systems, but also other processes at the enterprise, for example, the automated enterprise management system. Design process and comprehensive study play an important role in the creation of an automated security system, since at this stage all the qualitative characteristics of the future security system are laid down. The author analyzed modern trends and challenges in the market related to the implementation of automated security systems, as well as their impact on the level of security at an industrial enterprise. The main focus of the article is on the concept of integrating monitoring, control, and threat prediction technologies, which can significantly improve the effectiveness of risk management. The results of the study demonstrate that the implementation of automated systems helps to reduce the number of incidents, and increases the overall discipline and level of responsibility of employees.

Keywords: automation; integration; security system; enterprise; industrial enterprise processes

For citation: *A. Makeyev. AUTOMATED SECURITY SYSTEM FOR INDUSTRIAL ENTERPRISES// INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES. 2024. Vol. 5. No. 19. Pp. 115–127 (In Russ.). https://doi.org/10.54309/IJICT.2024.19.3.010.*

ӨНЕРКӘСІПТІК КӘСІПОРЫНДАРДЫ ҚОРҒАУДЫҢ АВТОМАТТАНДЫРЫЛҒАН ЖҮЙЕСІ

А. Макеев
ЖШС «Терралинк Технолоджис», Алматы, Қазақстан.
E-mail: alibekmakeyev@gmail.com

Алибек Макеев — ЖШС «Терралинк Технолоджис», талдаушысы, Алматы, Қазақстан
E-mail: alibekmakeyev@gmail.com, https://orcid.org/0009-0001-5174-825X.

Аннотация. Қауіпсіздік жүйелері қазіргі заманғы өнеркәсіптік кәсіпорындардың өмір сүруінің ажырамас бөлігіне айналды. Мұндай жүйе бірқалыпты жұмыс істеуі үшін жақсы жағдай жасап, бұл процесті автоматтандыру қажет. Заманауи қауіпсіздік жүйелерінің даму тенденциялары тек қауіпсіздік жүйелеріне ғана емес, сонымен қатар кәсіпорында бар басқа да процестерге, мысалы, кәсіпорынды басқарудың автоматтандырылған жүйесіне әсер ететін кең таралған автоматтандыру мен интеграцияға тікелей байланысты. Автоматтандырылған қауіпсіздік жүйелерін құруда маңызды рөлді жобалау және бар нюанстарды жан-жақты зерттеу процесі атқарады, өйткені дәл осы кезеңде болашақ қауіпсіздік жүйесінің барлық сапалық сипаттамалары белгіленеді. Автор автоматтандырылған қауіпсіздік жүйелерін енгізуге байланысты нарықтағы ағымдағы үрдістер мен қиындықтарды, сондай-ақ олардың өнеркәсіптік кәсіпорындағы қауіпсіздік деңгейіне әсерін талдаған. Мақаланың негізгі бағыты тәуекелдерді басқару тиімділігін айтарлықтай арттыра алатын мониторинг, бақылау және қауіптерді болжау технологияларын біріктіру тұжырымдамасына арналған. Зерттеу нәтижелері автоматтандырылған жүйелерді енгізу оқыс оқиғалардың санын азайтуға көмектесетінін, сонымен қатар қызметкерлердің жалпы тәртібі мен жауапкершілігін арттыратынын көрсетті.

Түйін сөздер: автоматтандыру; интеграция; қауіпсіздік жүйесі; кәсіпорын; өнеркәсіптік кәсіпорынның процестері

Дәйексөз үшін: *А. Макеев. ӨНЕРКӘСІПТІК КӘСІПОРЫНДАРДЫ ҚОРҒАУДЫҢ АВТОМАТТАНДЫРЫЛҒАН ЖҮЙЕСІ // ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ. 2024. Т. 5. No. 19. 115–127 бет. (орыс тілінде). https://doi.org/10.54309/IJICT.2024.19.3.010.*

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

А. Макеев
ТОО «Терралинк Технолоджис», Алматы, Казахстан.
E-mail: alibekmakeyev@gmail.com

Алибек Макеев — аналитик, ТОО «Терралинк Технолоджис»
E-mail: alibekmakeyev@ gmail.com, https://orcid.org/0009-0001-5174-825X.

Аннотация. Системы обеспечения безопасности стали неотъемлемой частью существования современных промышленных предприятий. Для того, чтобы такая система функционировала бесперебойно, необходимо создать лучшие условия и автоматизировать данный процесс. Тенденции развития современных систем безопасности напрямую имеют связь с широкой автоматизацией и интеграцией, которые затрагивают не только системы безопасности, но и остальные существующие на предприятии процессы, например, автоматизированные системы управления предприятия. Важную роль при создании автоматизированной системы обеспечения безопасности играет процесс проектирования и всестороннего изучения существующих нюансов, поскольку именно на этом этапе заложены все качественные характеристики будущей системы безопасности. Автор проанализировал современные тенденции и вызовы на рынке, связанные с внедрением автоматизированных систем обеспечения безопасности, а также их влияние на уровень безопасности на промышленном предприятии. Основное внимание в статье направлено на концепцию интеграции технологий мониторинга, контроля и предвидение угроз, что позволяет существенно повысить эффективность управления рисками. Результаты исследования демонстрируют, что внедрение автоматизированных систем способствует снижению числа инцидентов, а также повышает общую дисциплину и уровень ответственности сотрудников.

Ключевые слова: автоматизация; интеграция; система обеспечения безопасности; предприятие; процессы промышленного предприятия

***Для цитирования**: А. Макеев. АВТОМАТИЗИРОВАННАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ // МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ. 2024. Т. 5. No. 19. Стр. 115–127 (На русс.). https://doi.org/10.54309/IJICT.2024.19.3.010.*

Введение

Актуальность данной темы обусловлена тем, что в последние годы постоянно возрастает число инцидентов, связанных с нарушениями безопасности на крупных промышленных предприятиях. Это включает в себя как физические угрозы безопасности, так и систематические кибератаки, а также иные различные риски. Поэтому создание эффективной автоматизированной системы для обеспечения безопасности становится особенно важным. Увеличение числа киберугроз и физической преступности ставит промышленные предприятия перед необходимостью внедрения современных систем

безопасности, а в свою очередь, атаки на промышленные объекты могут привести к значительным экономическим потерям и поставить под угрозу жизни людей. Внедрение таких технологий в систему безопасности промышленного предприятия, как искусственный интеллект и машинное обучение, открывает новые возможности для повышения уровня безопасности на предприятиях.

Целью статьи на тему «Автоматизированная система обеспечения безопасности промышленных предприятий» выступает проведение анализа наиболее актуальных технологий и методик, которые используются прежде всего для обеспечения безопасности на промышленных объектах, с целью выявления оптимальных и актуальных решений для автоматизации систем безопасности.

Исходя из цели статьи, вытекают следующие основные задачи:

1. Исследование существующих систем обеспечения безопасности на промышленных предприятиях;
2. Определение ключевых требований к автоматизации систем обеспечения безопасности;
3. Разработка рекомендаций по внедрению автоматизированной системы обеспечения безопасности.

Гипотеза исследования заключается во внедрении автоматизированной системы обеспечения безопасности на промышленных предприятиях, что в свою очередь позволяет значительно снизить риски инцидентов, связанных с производственными авариями, киберугрозами и другими негативными факторами, которые могут возникнуть в функционировании предприятия, благодаря автоматизации и интеграции современных технологий мониторинга, анализа данных и оперативного реагирования.

Разработка гипотезы в данном случае основана на предположении о том, что автоматизированная система безопасности не только способствует улучшению контроля над производственными процессами на промышленном предприятии, но также способствует более эффективному использованию ресурсов предприятии, а вместе с тем и оптимизации затрат и повышению уровня защиты других его систем.

Методы и материалы

В статье использован такой метод, как анализ существующих систем безопасности на промышленных предприятий посредством изучения литературы по теме, а также проведен сравнительный анализ в виде оценки разных подходов к обеспечению безопасности промышленных предприятий. Среди материалов использованы: научные статьи и журналы по теме; учебные пособия.

Основная часть. На данный момент современные крупные промышленные предприятия сталкиваются с огромным количеством угроз, как внутренних, так и внешних. Эти угрозы могут иметь разный характер, начиная от несчастных случаев и утечек информации до террористических актов и атак на компьютерные системы. Поэтому на сегодняшний день возрастает реальная необходимость создание наиболее эффективной системы обеспечения безопасности, которая будет грамотно автоматизирована и интегрирована на предприятии (Абалмазов, 2023). В этом контексте автоматизированные системы обеспечения безопасности представляют собой важный инструмент, который позволяет интегрировать различные аспекты безопасности и управлять данными аспектами в единой информационной среде.

Автоматизированные системы обеспечения безопасности промышленных предприятий представляют собой целостный комплекс технических и программных

средств, предназначенных для защиты объектов от различных угроз, включая несанкционированный доступ, пожары, аварии, террористические акты и другие риски. Такие системы предназначены для повышения уровня безопасности, защиты персонала и имущества, а также для обеспечения выполнения нормативных требований.

Полноценная система безопасности промышленного предприятия включает в себя в том числе и мероприятия, которые обеспечивают защиту не только конфиденциальной информации, но и бизнес-процессов. Поэтому сюда же входят сохранность важных документов, обеспечение контроля доступа на предприятие, противодействие незаконной деятельности, например краже и т. д. (Буч и др., 2018).

В связи с этим, автоматизированная система обеспечения безопасности заключается не только в информационной безопасности и противодействии угрозам хакеров, но и в поддержке всех мероприятий, которые не связаны с информацией.

Промышленные сети автоматизации и управления играют ключевую роль в современных производственных процессах. Они обеспечивают связь между различными элементами системы управления, такими как датчики, контроллеры и исполнительные механизмы. Однако с увеличением сложности этих сетей возрастает и риск возникновения различных угроз, как внешних, так и внутренних.

К методам обеспечения промышленных сетей автоматизации и управления на предприятии можно отнести:

1. Использование в работе промышленного предприятия современных протоколов безопасности для защиты сетей, например: TLS/SSL; VPN; механизмы аутентификации и авторизации;
2. Полноценная разработанная система мониторинга, качественно внедренная в работу предприятия с целью своевременного обнаружения источников угроз и рисков, выявляя аномалии в реальном времени;
3. Внедрение в работу предприятия искусственного интеллекта, который в работе может сыграть ключевую роль, поскольку таким способом анализ большого количества данных будет проходить быстрее, отсюда следует и то, что потенциальные угрозы для промышленного предприятия будут найдены гораздо быстрее. Также с помощью использования искусственного интеллекта может произойти заблаговременное предотвращение возможных инцидентов;
4. Обучение персонала, поскольку именно человеческий фактор выступает как основная причина инцидентов безопасности, и поэтому обучение сотрудников на регулярной основе поможет значительно снизить риски (Галатенко, 2019).

Для того, чтобы обеспечить на промышленном предприятии полноценную безопасность, большинство руководителей используют целый комплекс ресурсов, которые включают в себя: материальные ресурсы; кадры; информационные ресурсы; технические ресурсы; правовые и нормативные ресурсы. На рисунке 1 рассмотрим основные моменты обеспечения системы безопасности на промышленном предприятии:

Рис.1 – Система безопасности объекта

К компонентам автоматизированной системы безопасности промышленных предприятий можно отнести три основных компонента. Первый компонент – это физическая безопасность. В неё входят такие компоненты, как контроль доступа, а также сигнализация и видеонаблюдение. Контроль доступа — это использование сложных или простых биометрических систем, пропусков и видеонаблюдения для управления входом на территорию промышленного предприятия. Сигнализация и видеонаблюдение — это совокупные системы, которые позволяют отслеживать попытки доступа посторонними людьми, а также осуществлять мониторинг территории предприятия в режиме реального времени.

Второй компонент – это информационная безопасность, в которую входит защита сети и управление данными. Защита сети — это использование антивирусных программ и систем обнаружения вторжений для обеспечения кибербезопасности информационных систем предприятия и предотвращение взлома с целью захвата информации. Управление данными — это защита конфиденциальной информации предприятия, а также шифрование важных данных и внедрение протоколов безопасности.

Третий компонент – это производственная безопасность, в который входит мониторинг технологических процессов предприятия и налаженные системы оповещения. Мониторинг технологических процессов — это использование специальных датчиков и автоматизированных систем для контроля за производственными процессами с целью предотвращения аварий и различных несанкционированных инцидентов. Системы оповещения — это автоматические системы оповещения о чрезвычайных ситуациях, с помощью которых представляется возможным быстро информировать сотрудников о возникших угрозах безопасности на предприятии (Домарев, 2020). На рисунке 2 рассмотрим подсистему обнаружения

атак автоматизированной системы безопасности:

Рис. 2 – Подсистема обнаружения атак автоматизированной системы безопасности

Исходя из рисунка 2, выделим ключевые преимущества автоматизированной системы безопасности на промышленном предприятии: интеграция информации, что позволяет значительно повысить эффективность рабочих процессов и избежать дублирования усилий; снижение рисков на предприятии, поскольку автоматизация позволяет гораздо быстрее реагировать на инциденты в реальном времени, минимизируя при этом риски для оборудования и персонала; улучшение мониторинга угроз и рисков, поскольку автоматизированные системы безопасности предприятия и их современные элементы позволяют соответствующим отделам предприятия проводить анализ возникших ранее инцидентов, а вместе с тем выявлять наиболее уязвимые места, способствуя постоянному улучшению системы безопасности; снижение затрат благодаря автоматизации процессов системы безопасности, что в разы сокращают расходы на безопасность (Зильбербург и др., 2020).

Также следует обратить внимание на большое количество видов систем обеспечения безопасности предприятия. Система контроля доступа, в которую можно отнести биометрические системы, карты доступа. Такие системы помогают предотвращать несанкционированный вход на предприятие и проводить учет посещаемости. Также они контролируют доступ сотрудников предприятия и гостей в определенные зоны (Иващенко и др., 2019).

Системы видеонаблюдения, которые включают в себя камеры видеонаблюдения, системы звуковой записи и передачи данных, что в свою очередь позволяет более точечно контролировать происходящее на территории предприятия. Такая система помогает выявлять совершенные правонарушениях, инцидентов и служат доказательством в случае чрезвычайных ситуаций.

Системы сигнализации, которые в свою очередь помогают обнаружить несанкционированные проникновения на территорию промышленного предприятия и могут включать в себя и датчики движения, разбития стекол, так и новейший интеллектуальные технологии. Благодаря подобным системам происходит мгновенное уведомление охраны о возможной угрозе предприятию и его имуществу.

Системы мониторинга и управления, которые помогают контролировать внутреннее состояние оборудования и всех производственных процессов, также такие

системы могут выполнять интегрированные функции безопасности процессов. Их полезность обусловлена оперативным реагированием на технические сбои и аварии.

Системы пожарной безопасности, которые составляют основу безопасности любого крупного промышленного предприятия. Включают в себя такие важные системы, как: обнаружение дыма, автоматическое тушение огня, оповещение об экстренной эвакуации. Такие системы защищают предприятие от серьезных угроз, при этом минимизируя риски для жизней людей, а также материальных ценностей.

Системы кибербезопасности внедряются с целью обеспечения защиты от атак со стороны хакеров, а также проводят мониторинг сетевой активности и тем самым предотвращают возможную утечку важных данных. Польза от подобных систем заключается в том, что они являются важным элементом защиты важных данных, систем и информации предприятия (Ивашкин, 2020).

Согласно отчету по безопасности на рабочих местах от МОТ, 30 % всех несчастных случаев на производстве можно предотвратить с помощью современных технологий безопасности. Исследование компании «Gartner» показало, что компании, внедряющие автоматизированные системы безопасности, могут сократить расходы на безопасность до 25 % в течение трех лет.

Во время автоматизации системы безопасности промышленного предприятия, представляется возможность контроля всей работы отделов компании. Также автоматизация позволяет значительно сократить количество работников, поскольку более опасные и емкие операции по предотвращению рисков и угроз безопасности можно возложить на машины и механизмы с элементами автоматики, повышая при этом безопасность и производительность труда у работников. В целом, сущность использования автоматизированных систем обеспечения безопасности на промышленном предприятии можно продемонстрировать на рисунке 3:

Рис. 3 - Сущность использования автоматизированных систем обеспечения безопасности на промышленном предприятии

Если рассмотреть примеры по реализации автоматизированных систем безопасности, то здесь можно рассмотреть компанию ООО «Северсталь» - гигант, который выходит далеко за пределы Российской Федерации. Используя автоматизированную систему обнаружения пожара, компания сумела значительно снизить количество ложных срабатываний, а именно на 40 %, что позволило в разы сократить время реакции на более реальные угрозы.

Другая компания, Ford, которая находится в Кракове, внедрила системы видеонаблюдения с полным анализом данных. Это позволило руководству уменьшить в разы количество краж и порчи имущества компании на 30 % всего за первый год эксплуатации.

На некоторых зарубежных предприятиях, например, Bosch, давно внедрены роботизированные системы безопасности компании с целью мониторинга окружающей среды в потенциально опасных зонах, что позволило снизить казусы на 20 % (Информационная безопасность автоматизированных систем: понятие, методы обеспечения)

Автоматизированные системы обеспечения безопасности становятся необходимым элементом в деятельности промышленных предприятий. Их внедрение позволяет не только защищать ресурсы, но и оптимизировать процессы управления и повысить общую эффективность работы. С учетом растущих угроз, автоматизированные системы безопасности являются важнейшим аспектом стратегического планирования и развития бизнеса современного промышленного предприятия.

Система безопасности предприятия должна развиваться вместе с предприятием и адекватно реагировать на разнообразные угрозы извне. На основе глубокого анализа изменений бизнес-процессов промышленного предприятия, а также внешней среды, должна меняться и модернизироваться и система его безопасности. Проанализировав современные угрозы и риски, которым подвергаются производство на промышленном предприятии, показал, что традиционные подходы к обеспечению системы безопасности не всегда являются эффективными (Кузнецов, 2019) В условиях быстрого развития технологий и нарастания сложности потенциальных угроз возрастает необходимость внедрения автоматизированных систем, способных оперативно реагировать на изменения в окружающей среде и обеспечивать безопасность на всех уровнях.

Результаты и обсуждение

Результаты данного исследования демонстрируют положительное влияние на промышленное предприятие внедрения автоматизированных систем обеспечения безопасности. Это повышает производительность и способствует повышению качества мониторинга и контроля безопасности.

На сегодняшний день многие промышленные предприятия сталкиваются с недостаточной эффективностью традиционных методов обеспечения безопасности как внутренней, так и внешней, что подчеркивает необходимость внедрения автоматизированных систем, способных обеспечить более высокий уровень защиты данных предприятия. В ходе исследования были рассмотрены ключевые компоненты, принципы и технологии, применяемые в автоматизированных системах, включая адаптивные системы мониторинга, аналитические инструменты, а также системы раннего реагирования.

В ходе обсуждения основных результатов исследования важно отметить, что автоматизация процессов обеспечения безопасности на промышленных предприятиях имеет ряд значительных преимуществ. Прежде всего, это повышает уровень безопасности за счет быстрого реагирования на инциденты и снижения человеческого фактора. Разработанные алгоритмы показали свою эффективность в обнаружении аномалий, что позволяет заранее принимать меры системы безопасности предприятия против угроз (Gartner, 2021).

Однако, помимо преимуществ, существуют и угрозы при реализации автоматизированной системы обеспечения безопасности. Во-первых, это возрастание

киберугроз, которая обусловлена тем, что система, которая работает на основе цифровых, то есть передовых, технологий, может стать главной мишенью атак хакеров, а это опасно в случае с промышленным предприятием, поскольку может подорвать весь производственный процесс. Именно поэтому необходимо учесть постоянное обновление системы и поддержки актуальности её защиты от угроз.

Во-вторых, это затраты на обучение персонала. Поскольку новая внедренная система требует от сотрудников соответствия по части знаний, это весьма затратно не только в материальном плане, но и в плане времени. Поэтому важно находить эффективные тренинги и программы по повышению квалификации с целью качественной и безопасной эксплуатации введенной системы.

В-третьих, происходит постоянная интеграция уже с существующими системами. Это связано с тем, что на многих промышленных предприятиях уже давно существуют определенные системы безопасности, и поэтому возникает необходимость в обеспечении объединения, или интеграции, новой автоматизированной системы безопасности с существующими ранее моделями.

В-третьих, существуют и морально-этические аспекты. К ним относятся такие спорные моменты, когда, например, использование новых автоматизированных технологий мониторинга могут вызвать вопросы о свободе труда сотрудников и поэтому возникает тонкая грань между нарушением прав сотрудников и использованием новейших автоматизированных систем безопасности.

Представленные результаты исследования подчеркивают значимость автоматизации процессов обеспечения безопасности на промышленных предприятиях и открывают новые горизонты для дальнейших научных исследований и практических разработок в этой области. Внедрение эффективных и современных автоматизированных систем станет залогом повышения уровня безопасности, устойчивости и конкурентоспособности промышленных предприятий в условиях динамично развивающегося рынка.

Данное комплексное исследование показало, что автоматизированные системы обеспечения безопасности, такие, например, как системы видеонаблюдения, контроля доступа, а также системы обнаружения возгораний и утечек, способны значительно повысить уровень безопасности на промышленных объектах, при этом повысив его производительность. Кроме того, интеграция данных систем в единую платформу позволяет оптимизировать процессы мониторинга и управления, что в свою очередь снижает риск ошибок, связанных с человеческим фактором.

На основе проведенного анализа можно сделать ряд рекомендаций по дальнейшему совершенствованию автоматизированных систем безопасности. Важными направлениями являются: развитие адаптивных систем, способных к самонастройке в зависимости от меняющихся условий; использование искусственного интеллекта для повышения скорости анализа и принятия решений; а также обеспечение высокого уровня киберзащиты для защиты систем от внешних угроз.

Заключение

В заключении хочется отметить то, что автоматизированные системы обеспечения безопасности в настоящий момент становятся необходимостью для современных промышленных предприятий. Промышленные предприятия выступают как ключевые объекты в экономике, однако зачастую они подвержены различным видам рисков. Традиционные методы обеспечения безопасности не всегда выступают

как эффективные способы обеспечения уровня безопасности, именно поэтому автоматизированные системы могут значительно повысить уровень защиты, улучшить реакцию на инциденты и оптимизировать процессы управления безопасностью. Они позволяют не только защищать активы предприятия в целостности, но также и снизить риски, создавая при этом наиболее безопасную производственную среду для сотрудников различных отделов. В условиях современных вызовов и угроз, внедрение автоматизированных систем безопасности на промышленное предприятие является стратегическим шагом, позволяющим современным предприятиям уверенно смотреть в будущее.

Основные выводы работы можно сформулировать следующим образом:

1. Автоматизированные системы обеспечения безопасности на промышленном предприятии способны обеспечить более высокий уровень контроля и управления по сравнению с традиционными системами безопасности, что позволяет значительно снизить риски инцидентов и аварий на производстве, тем самым повышая производительность труда;

2. Внедрение таких систем обеспечения безопасности способствует повышению эффективности управления безопасностью на предприятии за счет интеграции различных видов систем безопасности и аналитических инструментов, позволяющих в реальном времени отслеживать ситуацию и принимать оперативные решения;

3. Важно учитывать человеческий фактор и обеспечивать необходимую подготовку персонала для работы с новыми технологиями, что является критическим условием успешного внедрения автоматизированных систем;

4. Перспективы дальнейших исследований включают разработку более сложных алгоритмов машинного обучения для прогноза возможных угроз, а также интеграцию с системами управления производственными процессами для создания единой среды управления безопасностью на промышленном предприятии.

Также нужно отметить то, что в современных условиях рыночной экономики, промышленные предприятия сталкиваются с многочисленными угрозами, включая угрозы физической безопасности, киберугрозы и экологические риски. В данной статье представлена разработка автоматизированной системы обеспечения безопасности на промышленном предприятии, которая способна интегрировать и довести до автоматизации современные технологии для предотвращения инцидентов и минимизации любых возникающих угроз, рисков и последствий. Описываются ключевые компоненты системы, методы анализа рисков, а также примеры внедрения с использованием реальных данных.

Также следует отметить тот факт, что автоматизированные системы обеспечения безопасности имеют потенциал значительно улучшить ситуации на промышленных предприятиях. Однако успешная реализация требует комплексного подхода, включая технические, организационные и морально-этические аспекты. Предстоит дальнейшее исследование и адаптация систем к меняющимся условиям и требованиям.

Обеспечение безопасности и надежности промышленных сетей автоматизации и управления является сложной задачей, требующей комплексного подхода. Использование современных технологий, внедрение систем мониторинга, а также обучение персонала могут существенно повысить уровень защиты предприятий от потенциальных угроз. Промышленные сети автоматизации и управления играют

ключевую роль в современных производственных процессах. Они обеспечивают связь между различными элементами системы управления, такими как датчики, контроллеры и исполнительные механизмы. Однако с увеличением сложности этих сетей возрастает и риск возникновения различных угроз, как внешних, так и внутренних.

ЛИТЕРАТУРА

Абалымазов Э.И. (2023). «Концепция безопасности: тактика высокоэффективной защиты. Стоимость стратегии, стратегические ресурсы, тактика защиты, сопоставимость тактических решений». — Системы безопасности. — 4. — 111–115.

АСПБ (Система управления промбезопасностью). [Электронный ресурс]. Режим доступа: https://smis-expert.com/aspb-sistema-upravleniya-prombezopasnostyu/, свободный (дата обращения: 18.09.2024).

Буч Г., Рамбо Дж., Джекобсон А. (2018). UML. Проектирование программных комплексов, информационных систем. — М.: ДМК Пресс, СПб.: Питер. — 432 с.

Галатенко В.А. (2019). Стандарты информационной безопасности / Под ред. В.Б. Бетелина. — М.: ИНТУИТ.РУ «Интернет-университет информационных технологий». — 328 с.

Домарев В.В. (2020). Безопасность информационных технологий. Методология создания систем защиты. — К.: ДиаСофт. — 614 с.

Зильбербург Л.И., Молочник В.И., Яблочников Е.И. (2020). Реинжиниринг и автоматизация технологической подготовки производства в машиностроении. — СПб.: Компьютербург. — 152 с.

Иващенко А.В., Кременецкая М.Е. (2019). Автореинжиниринг единого информационного пространства предприятия. — Самара: СНЦ РАН. — 116 с.

Ивашкин С.В. (2020). Методы защиты промышленных сетей. — М.: Научный мир.

Информационная безопасность автоматизированных систем: понятие, методы обеспечения. [Электронный ресурс]. Режим доступа: https://gb.ru/blog/informatsionnaya-bezopasnost-avtomatizirovannykh-sistem/, свободный (дата обращения: 18.09.2024).

Кузнецов Е.В. (2019). Автоматизация и управление на предприятии. — Екатеринбург: УралГТУ.

Медведовский И. (2018). «Современные методы и средства анализа и контроля рисков информационных систем компаний». iXBT.com. — 7. — 138–140.

Омельянчук А.М. (2018). «Формирование систем комплексной безопасности». Системы безопасности. — 1(85). — 100–102.

Об автоматизации процессов охраны труда в промышленности. [Электронный ресурс]. Режим доступа: https://www.cti.ru/media/publications/ob-avtomatizatsii-protsessov-okhrany-truda-v-promyshlennosti/, свободный (дата обращения: 18.09.2024).

Петров А.А. (2021). Информационная безопасность промышленности. — СПб.: Наука.

Резников Г.Я., Бабин С.А., Костогрызов А.И., Родионов В.Н. (2021). «Количественная оценка защищенности автоматизированных систем от несанкционированного доступа». Информационные технологии в проектировании и производстве. — 1. — 11–22.

Резников Г.Я. (2020). Рациональный мониторинг процессов менеджмента качества на предприятиях. — М.: Мир. — 284 с.

Садердинов А.А., Трайнев В.А., Федулов А.А. (2023). Информационная безопасность предприятия: Учебное пособие. — М.: Дашков и Ко. — 336 с.

Ярочкин В.И. (2021). Служба безопасности коммерческого предприятия. — М.: Ось-89. — 144 с.

International Labour Organization (ILO). (2021). Safety and Health at Work: — A Vision for Sustainable Prevention.

Gartner (2021). Market Guide for Security Information and Event Management.

REFERENCES

Abalmazov E.I. (2023). Kontseptsiya bezopasnosti: taktika vysokoeffektivnoy zashchity. Stoimost strategii, strategicheskie resursy, taktika zashchity, sopostavimost takticheskikh resheniy [Security concept: tactics of highly effective protection. Cost of strategy, strategic resources, defense tactics, comparability of tactical decisions]. — Sistemy bezopasnosti [Security Systems]. — 4. — 111–115. [In Russ.].

ASPB (Sistema upravleniya prombezopasnostyu). (2024). [Electronic resource]. Available at: https://smis-expert.com/aspb-sistema-upravleniya-prombezopasnostyu. — Accessed: 18 September 2024.

Buch G., Rambo Dzh., Dzhakobson A. (2018). UML. Proyektirovaniye programmnykh kompleksov, informatsionnykh sistem [UML. Design of software packages, information systems]. — Moscow: DMK Press, St. Petersburg: Piter. — 432 p. [In Russ.].

Galatenko V.A. (2019). Standarty informatsionnoy bezopasnosti [Information security standards]. Ed. V.B. Betelin. —Moscow: INTUIT.RU "Internet University of Information Technologies". — 328 p. [In Russ.].

Domarev V.V. (2020). Bezopasnost informatsionnykh tekhnologiy. Metodologiya sozdaniya sistem zashchity [Information technology security. Methodology for creating protection systems]. — Kyiv: DiaSoft. — 614 p. [In Russ.].

Zilberburg L.I., Molochnik V.I., Yablochnikov E.I. (2020). Reinzhiniring i avtomatizatsiya tekhnologicheskoy podgotovki proizvodstva v mashinostroyenii [Reengineering and automation of technological preparation of production in mechanical engineering]. — St. Petersburg: Kompyuterburg. — 152 p. [In Russ.].

Ivaschenko A.V., Kremenetskaya M.E. (2019). Avtoereinzhiniring yedinogo informatsionnogo prostranstva predpriyatiya [Autoreengineering of the unified information space of an enterprise]. — Samara: SRC RAS. — 116 p. [In Russ.].

Ivashkin S.V. (2020). Metody zashchity promyshlennykh setey [Methods of industrial network protection]. — Moscow: Nauchny Mir. [In Russ.].

Information security of automated systems: concept, methods of provision. (2024). [Electronic resource]. Available at: https://gb.ru/blog/informatsionnaya-bezopasnost-avtomatizirovannykh-sistem. —Accessed: 18 September 2024.

Kuznetsov E.V. (2019). Avtomatizatsiya i upravleniye na predpriyatii [Automation and management at the enterprise]. — Ekaterinburg: UralSTU. [In Russ.].

Medvedovsky I. (2018). "Sovremennyye metody i sredstva analiza i kontrolya riskov informatsionnykh sistem kompaniy" [Modern methods and means of analysis and control of risks in company information systems]. iXBT.com. — 7. — 138–140. [In Russ.].

Omelyanchuk A.M. (2018). "Formirovaniye sistem kompleksnoy bezopasnosti" [Formation of integrated security systems]. Sistemy bezopasnosti [Security Systems]. — 1(85). — 100–102. [In Russ.].

On the automation of labor protection processes in industry (2024). [Electronic resource]. Available at: https://www.cti.ru/media/publications/ob-avtomatizatsii-protsessov-okhrany-truda-v-promyshlennosti. — Accessed: 18 September 2024.

Petrov A.A. (2021). Informatsionnaya bezopasnost promyshlennosti [Information security of industry]. — St. Petersburg: Nauka. [In Russ.].

Reznikov G.Ya., Babin S.A., Kostogryzov A.I., Rodionov V.N. (2021). "Kolitsevnaya otsenka zashchishchennosti avtomatizirovannykh sistem ot nesanktsionirovannogo dostupa" [Quantitative assessment of the security of automated systems from unauthorized access]. Informatsionnyye tekhnologii v proyektirovanii i proizvodstve [Information Technologies in Design and Production]. — 1. — 11–22. [In Russ.].

Reznikov G.Ya. (2020). Ratsionalnyy monitoring protsessov menedzhmenta kachestva na predpriyatiyakh [Rational monitoring of quality management processes at enterprises]. — Moscow: Mir. — 284 p. [In Russ.].

Saderdinov A.A., Trainev V.A., Fedulov A.A. (2023). Informatsionnaya bezopasnost predpriyatiya: Uchebnoye posobiye [Information security of the enterprise: A tutorial]. — Moscow: Dashkov i Ko. — 336 p. [In Russ.].

Yarochkin V.I. (2021). Sluzhba bezopasnosti kommercheskogo predpriyatiya [Security service of a commercial enterprise]. — Moscow: Os-89. — 144 p. [In Russ.].

International Labour Organization (ILO). (2021). Safety and Health at Work: A Vision for Sustainable Prevention.

Gartner (2021). Market Guide for Security Information and Event Management.

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