DOI 10.52209/1609-1825_2022_1_311 УДК 004.75

Модели удаленного управления промышленными сетями

[1]**ЩЕРБОВ Александр Сергеевич,** *магистрант, alexandr.chsherbov@gmail.com,*
[1]**ЯВОРСКИЙ Владимир Викторович,** *д.т.н., профессор, yavorskiy-v-v@mail.ru,*
[1]***КЛЮЕВА Елена Георгиевна,** *старший преподаватель, e.klyueva@kstu.kz,*
[1]**КОККОЗ Махаббат Мейрамкызы,** *к.п.н., зав. кафедрой, makhabbat_k@bk.ru,*
[1]Карагандинский технический университет, Казахстан, 100027, Караганда, пр. Н. Назарбаева, 56,
**автор-корреспондент.*

Аннотация. *Цель исследования: провести анализ современных перспективных технологий для обеспечения удаленного доступа к бизнес-системам и технологическим подсистемам управления производством. Статья посвящена проблеме применения методов удаленного управления через Internet технологическими процессами на предприятии. В статье проводится анализ существующих решений, определяются основные достоинства данного подхода, а также дается оценка векторов угроз безопасности сетей Operational Technology (OT). Авторами предлагается ряд общих правил для обеспечения полного контроля и безопасности удаленного подключения. В заключении делается вывод об обоснованности использования удаленного доступа на промышленных предприятиях различного уровня.*

Ключевые слова: *удаленный доступ, сети Operational Technology, VPN, PAM, информационная безопасность, сетевые технологии.*

Введение

Для большинства пользователей обычным является использование Internet и информационных систем и сетей, в то же время использование промышленных или технологических сетей, не так широко распространено, хотя играет очень важную роль в производстве товаров и жизнедеятельности предприятий. Автоматизированные системы управления технологическими процессами (АСУТП) – это критическая часть производства, поскольку управление технологическими процессами становится всё более автоматизированным и связанным с бизнес-процессами и управлением, вплоть до полного контроля процессов менеджерами продаж, а не техническим персоналом.

В качестве примера можно привести системы управления производством (Manufacturing Execution Systems, MES) [1], которые в своей сущности подразумевают полную автоматизацию производства от формирования заказа, до отгрузки готовой продукции без вмешательства персонала.

Целью настоящего исследования является анализ технологий, используемых для обеспечения удалённого доступа к бизнес-системам и технологическим подсистемам управления производством, выявление их основных достоинств и недостатков, а также обоснование необходимости использования подобных технологий на промышленных предприятиях различного уровня.

Материалы и методы исследования

Промышленная сеть (ПС) представляет собой набор контроллеров, линий связей, серверов баз данных, серверов приложений и рабочих станций операторов [2]. ПС позволяет полностью контролировать процесс производства, изменять параметры производства, получать технологические показатели для отслеживания соответствия стандартам и увеличения выхода годного продукта, а также минимизации брака.

На рисунке 1 представлена типовая схема взаимодействия сетей Information Technology (IT) и Operational Technology (OT) [3].

IT-сети – это сети бизнес-данных и пользователей. Часто применяется определение «общедоступные сети», т.е. сети, в которых данные могут направляться в различных направлениях и использоваться всеми.

OT-сети – более закрытая часть производства. Потоки данных в таких сетях идут в строгом направлении с обязательным контролем правильности и достоверности, за что отвечают специальные механизмы контроля чётности и проверки хэша.

К сетям OT можно отнести системы АСУТП энергетических компаний, металлургических комбинатов, нефтехимических производств. В общем это те сети, которые закрыты для внешних пользователей и не имеют прямого доступа к общим сетям, в особенности к Internet.

Актуальность исследования обусловлена широким внедрением АСУТП на промышленных предприятиях Казахстана, Карагандинского региона, а также развитием концепции удаленной работы и технологий Internet.

В ходе исследования был проведен анализ подходов к организации удаленного управления

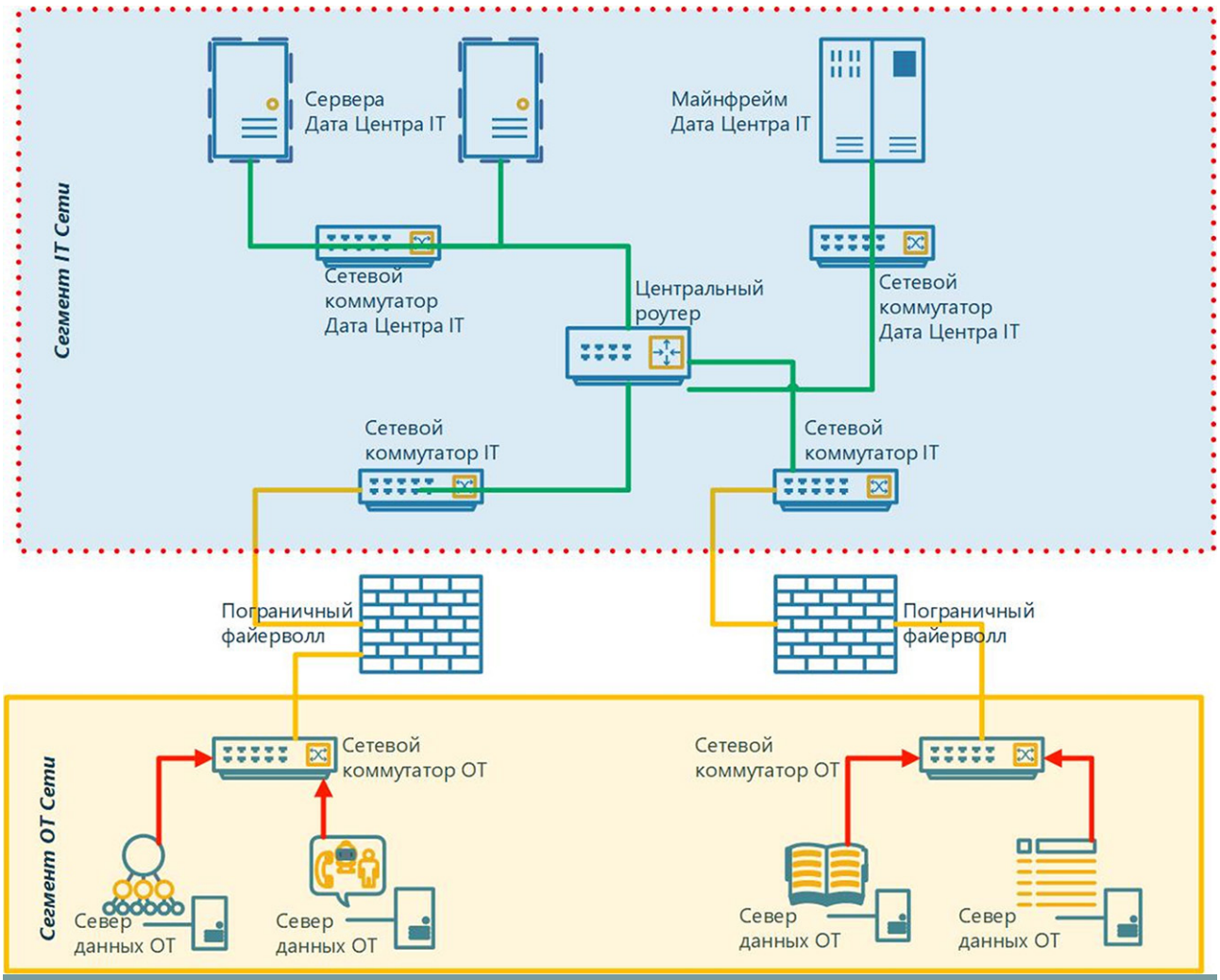

Рисунок 1 – Типовое построение и взаимодействие сетей IT и OT

сетями OT, были определены их основные достоинства для конечного предприятия, а также выявлены векторы угроз безопасности сетей OT. Опыт применения удаленного управления рассмотрен на примере АО «АрселорМиттал Темиртау». На основе полученных данных были определены общие правила для обеспечения полного контроля и безопасности подключения к АСУТП производственных предприятий.

Результаты и их обсуждение

Первоначальным протоколом передачи для сетей OT являлся протокол PROFIBUS [4], позволяющий объединить в единую систему различные разрозненные устройства автоматизации на физическом уровне. Однако его внедрение и применение требовало наличия специализированного оборудования (кабель, сетевые карты, сетевые коммутаторы), что вело к дополнительным затратам на построение фактически отдельной инфраструктуры. В связи с широким распространением Ethernet в сетях IT было разработано новое поколение протокола PROFIBUS – PROFINET [5], который позволяет использовать стандартное оборудование сетей IT для передачи технологических данных. Именно это развитие протокола позволило стереть грань между сетями IT и OT, сделав их, по сути, равнозначными и совместимыми.

В спецификации V2.3 механизмы Fast Forwarding, Dynamic Frame Packing и Fragmentation были определены как повышение производительности PROFINET, позволяющее сократить время цикла до 31,25 мкс с неограниченной параллельной передачей стандартных данных. Таким образом, PROFINET обеспечивает необходимую производительность для удовлетворения даже потенциальных будущих потребностей приложений.

Благодаря такой интеграции, появилась возможность прямого доступа к сетям OT из внешних сетей передачи данных, а также удалённого управления, что вызвало не только увеличение производительности и возможностей удалённой поддержки, но и выявило новые риски.

На основе проведенного в ходе исследования анализа были выявлены основные преимущества удалённого подключения и управления OT-сетями (таблица).

Приведённые примеры – это не полный список ситуаций, когда удалённый доступ к сетям OT необходим и эффективен. Быстрота доступа про-

Преимущества использования удаленного подключения и управления сетями ОТ	
Функция	**Преимущество**
Внедрение нового процесса	Как правило, требует нахождения на месте высококвалифицированного специалиста. Удалённый режим позволяет специалисту не присутствовать на месте, а находясь в офисе проводить необходимые изменения со своего компьютера.
Поддержка/контроль технологического процесса	Отпадает необходимость физического присутствия на площадке. Удалённый контроль позволяет полностью изменять параметры, вплоть до полной остановки процессов, в критических случаях.
Удалённый помощник	Подключение для проведения консультаций или корректировки технологического процесса. Зачастую используется для выполнения гарантийных обязательств.
Получение данных (метрик) работы оборудования и анализ технологических процессов	Всё более расширяется, в связи с использованием облачных технологий для бизнес-аналитики (BI).

изводителя или сервисной компании к оборудованию повышает надёжность производства, но в то же время появляются риски безопасности данных и целостности процессов.

В 2020 году одна из сервисных компаний в ЮАР была подвержена атаке промышленных хакеров. Компания обслуживала ряд крупных металлургических и горнодобывающих предприятий. Из-за отсутствия должного разделения и сегментирования сервисных сетей, а также недостаточного документирования технологических сетей заказчиков, злоумышленники получили доступ к управлению технологическим оборудованием и серверами баз данных. Общий ущерб от действий хакеров составил порядка 20 000 000 долларов США [6].

Сети ОТ достаточны уязвимы для атак, поскольку использование антивирусной защиты или установка обновлений операционных систем практически невозможна в силу специфики работы программного обеспечения. Порядка 90% технологических сетей до сих пор используют в качестве операционных систем Windows XP, Windows 7. В качестве серверных операционных систем – Windows 2000 [2].

Таким образом, к рискам внедрения удалённого доступа можно отнести следующие векторы угроз безопасности сетей ОТ:

- вирусы: отсутствие антивирусной защиты как в самой сети ОТ, так и на удалённых рабочих станциях может привести к потере данных или остановке производственных процессов;

- инсайдеры: персонал, который может выполнять злонамеренные действия по нарушению производственного процесса с целью нарушения цепочки производства;

- непреднамеренные действия: низкая квалификация персонала или непонимание процесса производства, которая может привести к нарушению производственного цикла;

- контроль информационной безопасности (ИБ): отсутствие процедур и политик при организации удалённого доступа как со стороны заказчика, так и со стороны исполнителя, может привести как к потере/изменению данных, так и потере контроля над производственным процессом.

Количество и качество рисков различно для каждой отдельно взятой сети или технологии, но можно определить ряд общих правил, которые должны быть внедрены для обеспечения полного контроля и безопасности подключения:

- подписание договора о неразглашении: базовая и обязательная часть соглашения об обслуживании с третьими лицами, в которой должны быть указаны максимально возможные варианты утечки информации и меры их предупреждения, а также меры воздействия;

- договор об ответственности: в отличие от предыдущего пункта, включает в себя конкретные положения и ответственность при проведении работ третьими лицами, их порядок и контроль;

- наличие политик и положений ИБ: должны быть разработаны и согласованы документы, описывающие полный процесс предоставления доступа, контроля, аудита выполняемых операций;

- чек-листы и процедуры контроля: наличие списков контроля, выполняемых и заполняемых на регулярной основе для подтверждения целостности процессов и данных;

- выполнение резервного копирования: на регулярной основе полные копии мастер проектов, исполняемых кодов, баз данных, настроек, документации;

- наличие плана Disaster Recovery: документации, резервных копий, запасного оборудования для осуществления аварийного восстановления;

- цепочка согласований (Request For Change): решение о предоставлении доступа или выполнения корректирующих действий в продуктивной системе должно приниматься минимально 3 людьми, различных департаментов для подтверждения необходимости проводимых действий.

Указанные мероприятия применимы в боль-

шинстве производственных секторов производства, но есть и достаточно специфичные правила для предприятий оборонной промышленности, государственного и банковского секторов, которые имеют более строгие требования и контроль в силу специфики выполняемых функций и социальной ответственности.

На рисунке 2 представлены основные векторы атак в период с января 2020 по июнь 2021 года по данным X-Force Incident Response Data [7]. В разрезе сетей ОТ таковыми являлись DDoS атаки (10%), кража учётных данных (13%), вымогатели (30%), трояны удалённого доступа (16%), инсайдеры (11%).

В отношении векторов первоначального заражения данные X-Force по реагированию на инциденты показывают, что эксплуатация уязвимостей и кража учетных данных являются наиболее распространенными точками входа для противников, что привело к 40 и 32% устраненных инцидентов, соответственно (рисунок 3).

Несмотря на достаточно существенные риски при правильной организации удалённый доступ к сетям ОТ становится нормой и действенным решением по осуществлению удалённого управления и мониторинга для повышения качества производственных процессов и их стабильности.

Финансовая составляющая решения по удалённому доступу состоит из многих факторов, однако нужно принимать во внимание, что решения Virtual Private Network (VPN) [8] или Privileged Access Management (PAM) [9] могут использоваться не только для сетей ОТ, но и для целей предприятия по оптимизации бизнес-процессов, что в свою очередь снижает совокупную стоимость владения (Total Cost of Ownership, TCO) [10].

Например, стоимость решения для построения VPN варьируется от 10 000 до 30 000$. В некоторых случаях при использовании существующей виртуальной среды и продуктов Open Source (Zentyal, PfSense и другие) можно получить нулевую стоимость внедрения. В этом плане решение остается за компанией с учетом принятия рисков, обучения персонала и осуществления контроля.

Решения PAM дешевле, но лицензируются по точкам подключения. Например, на 10 конечных точек подключения, стоимость внедрения составит 10 000 $. При этом появляется возможность практически 100% контроля выполняемых действий, аудита подключений и контроля запускаемых программ.

В то же время, при традиционном обслуживании систем с выездом специалиста на площадку заказчика, расходы в среднем составляют 100 $ в день, а время выполнения работ 7 дней. Таким образом, работа одного инженера в неделю обходится компании в 700 $. При этом эффективность его нахождения на производственной площадке зачастую весьма условна.

АО «АрселорМиттал Темиртау» имеет 10 контрактов с обслуживающими организациями для удалённой поддержки процессов и оборудования. Специалистами компании были внедрены многоуровневые решения VPN для минимизации угроз. В комплексе с решениями PAM специалисты «АрселорМиттал Темиртау» могут полностью контролировать подключения и выполняемые действия третьих сторон.

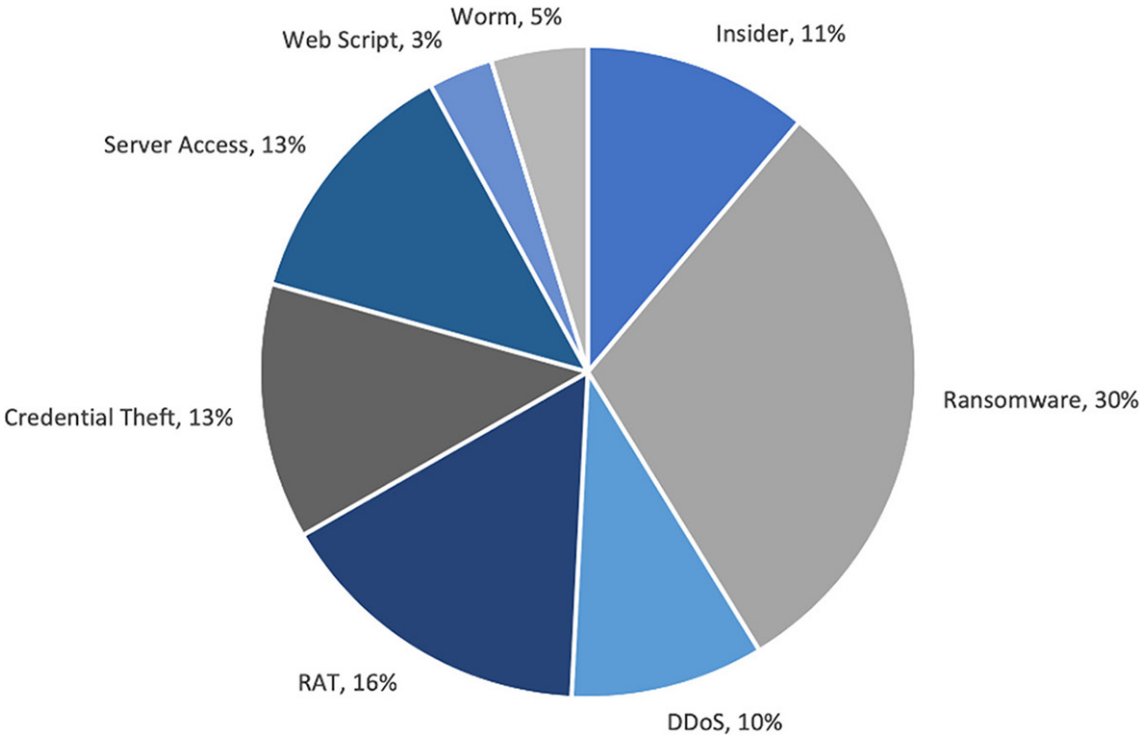

Рисунок 2 – Типы атак на организации, подключенные к сетям ОТ, январь 2020 – июнь 2021 года

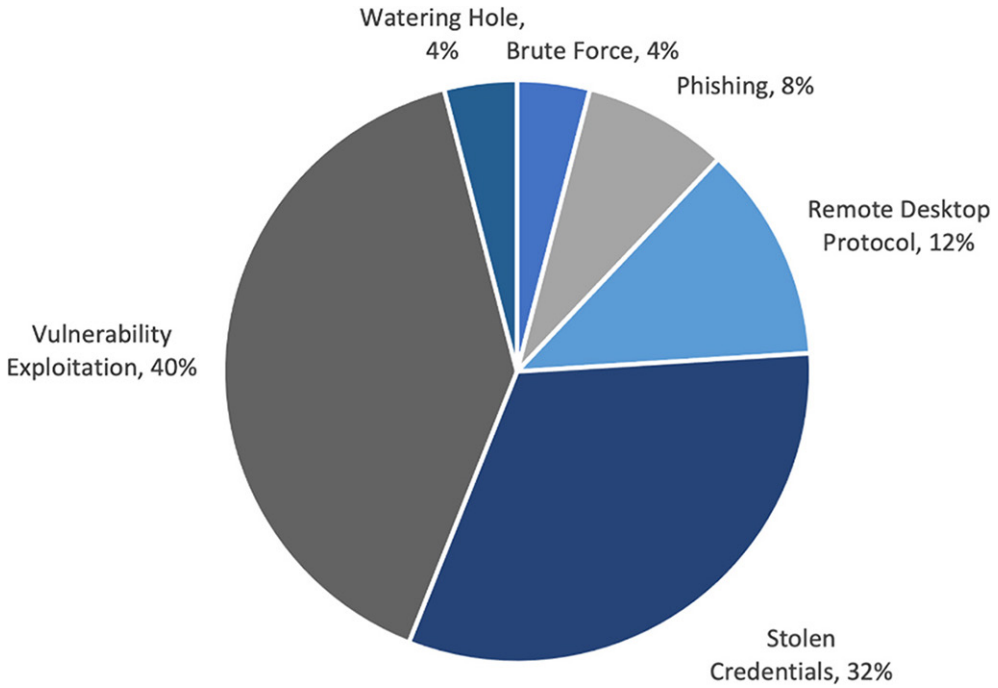

Рисунок 3 – Начальные векторы заражения, используемые в атаках на организации, подключенные к сетям ОТ, январь 2020 – июнь 2021 года

Заключение

Исходя из проведенного анализа можно сделать вывод, что решение о внедрении удалённого доступа к сетям ОТ для обслуживания третьими сторонами является наиболее экономически и функционально выгодным для предприятий, за исключением случаев, когда предоставление удалённого доступа не может быть осуществлено по техническим или иным причинам.

Удалённое управление технологическими устройствами с целью корректировки параметров или контроля работы оборудования – это новая тенденция в обслуживании удалённых технологических объектов, которая становится нормой и услугой стороннего обслуживания, позволяет использовать высококвалифицированные инженерные ресурсы не только инжиниринговых компаний, но и производителей оборудования.

СПИСОК ЛИТЕРАТУРЫ

1. Manufacturing Execution Systems Reviews and Ratings. – Текст: электронный // Gartner peerinsights: [сайт]. – URL: https://www.gartner.com/reviews/market/manufacturing-execution-systems (дата обращения: 17.09.2021).
2. Смычек, М.А. Технологические сети и системы связи: Учебное пособие / М.А. Смычек. – Вологда: Инфра-Инженерия, 2019. – 400 с.
3. Operational technology (OT) – definitions and differences with IT. – Текст: электронный // I-SCOOP: [сайт]. – URL: https://www.i-scoop.eu/industry-4-0/operational-technology-ot/ (дата обращения: 20.09.2021).
4. PROFIBUS. – Текст: электронный // PROFIBUS. PROFINET: [сайт]. – URL: https://www.profibus.com/technology/profibus (дата обращения: 28.09.2021).
5. PROFINET – the leading Industrial Ethernet Standard. – Текст: электронный // PROFIBUS. PROFINET: [сайт]. – URL: https://www.profibus.com/technology/profinet (дата обращения: 28.09.2021).
6. Кибербезопасность в сфере геологоразведки и добычи нефти и газа. – Текст: электронный // Deloitte: [сайт]. – URL: https://www2.deloitte.com/ru/ru/pages/energy-and-resources/articles/tracking-the-trends-2020/2017/cybersecurity-for-upstream-oil-and-gas.html (дата обращения: 04.10.2021).
7. X-ForceThreatIntelligenceResearchHub. – Текст: электронный // IBM: [сайт]. – URL: https://www.ibm.com/security/xforce/research-hub (дата обращения: 07.10.2021).
8. VPN-решения для корпоративных сетей. – Текст: электронный // TADVISER: [сайт]. – URL: https://www.tadviser.ru/index.php/Статья:VPN-решения_для_корпоративных_сетей (дата обращения: 17.11.2021).
9. Ellen, Neveux Why Privileged Access Management (PAM) Isn't the Ideal Solution for Managing Vendors / Neveux Ellen. – Текст: электронный // SecureLink: Third-Party Security: [сайт]. – URL: https://www.securelink.com/blog/why-privileged-access-management-pam-is-not-the-ideal-solution-for-managing-vendors/ (дата обращения: 09.10.2021).
10. Total Cost of Ownership in Technology: Implementation. – Текст: электронный // TechnologyAdvise: [сайт]. – URL: https://technologyadvice.com/blog/sales/total-cost-ownership-crm-marketing-automation/ (дата обращения: 02.11.2021).

Өндірістік желілерді қашықтан басқару модельдері

[1]***ЩЕРБОВ Александр Сергеевич,*** *магистрант, alexandr.chsherbov@gmail.com,*
[1]***ЯВОРСКИЙ Владимир Викторович,*** *т.ғ.д., профессор, yavorskiy-v-v@mail.ru,*
[1]****КЛЮЕВА Елена Георгиевна,*** *аға оқытушы, e.klyueva@kstu.kz,*
[1]***КОККОЗ Махаббат Мейрамкызы,*** *п.ғ.к., кафедра меңгерушісі, makhabbat_k@bk.ru,*
[1]*Қарағанды техникалық университеті, Қазақстан, 100027, Қарағанды, Н. Назарбаев даңғылы, 56,*

**автор-корреспондент.*

Аңдатпа. *Зерттеудің мақсаты: бизнес жүйелеріне және өндірісті басқарудың технологиялық ішкі жүйелеріне қашықтан қол жеткізуді қамтамасыз етудің заманауи перспективалық технологияларын талдау. Мақала кәсіпорындағы технологиялық процестерді интернет арқылы қашықтан басқару әдістерін қолдану мәселесіне арналған. Мақалада қолданыстағы шешімдер талданады, осы тәсілдің негізгі артықшылықтары анықталады, сонымен қатар Operational Technology (OT) желілерінің қауіпсіздігіне қауіп векторларына баға беріледі. Авторлар қашықтағы қосылымдардың толық бақылауы мен қауіпсіздігін қамтамасыз ету үшін бірқатар жалпы ережелерді ұсынады. Қорытындылай келе, әртүрлі деңгейдегі өнеркәсіптік кәсіпорындарда қашықтан қол жеткізуді пайдалану орынды деген қорытындыға келді.*

Кілт сөздер: *қашықтан қол жеткізу, Operational Technology желілері, VPN, PAM, ақпараттық қауіпсіздік, желілік технологиялар.*

Models of Remote Management of Industrial Networks

[1]***SHCHERBOV Alexandr,*** *master student, alexandr.chsherbov@gmail.com,*
[1]***YAVORSKIY Vladimir,*** *Dr. of Tech. Sci., Professor, yavorskiy-v-v@mail.ru,*
[1]****KLYUYEVA Yelena,*** *Senior Lecturer, e.klyueva@kstu.kz,*
[1]***KOKKOZ Makhabbat,*** *Cand. of Ped. Sci., Head of Department, makhabbat_k@bk.ru,*
[1]*Karaganda Technical University, Kazakhstan, 100027, Karaganda, N. Nazarbayev Avenue, 56,*

**corresponding author.*

Abstract. *Purpose of the study: to analyze modern promising technologies for providing remote access to business systems and technological subsystems of production management. The article is devoted to the problem of using methods of remote control over the Internet of technological processes in an enterprise. The article analyzes existing solutions, identifies the main advantages of this approach, and also provides an assessment of the vectors of threats to the security of Operational Technology (OT) networks. The authors propose a number of general rules to ensure complete control and security of remote connections. In conclusion, it is concluded that the use of remote access at industrial enterprises of various levels is reasonable.*

Keywords: *remote access, Operational Technology networks, VPN, PAM, information security, network technologies.*

REFERENCES

1. Manufacturing Execution Systems Reviews and Ratings. – Tekst: elektronnyj // Gartner peerinsights: [sajt]. – URL: https://www.gartner.com/reviews/market/manufacturing-execution-systems (data obrashcheniya: 17.09.2021).
2. Smychek, M.A. Tekhnologicheskie seti i sistemy svyazi: Uchebnoe posobie / M.A. Smychek. – Vologda: Infra-Inzheneriya, 2019. – 400 c.
3. Operational technology (OT) – definitions and differences with IT. – Tekst: elektronnyj // I-SCOOP: [sajt]. – URL: https://www.i-scoop.eu/industry-4-0/operational-technology-ot/ (data obrashcheniya: 20.09.2021).
4. PROFIBUS. – Tekst: elektronnyj // PROFIBUS. PROFINET: [sajt]. – URL: https://www.profibus.com/technology/profibus (data obrashcheniya: 28.09.2021).
5. PROFINET – the leading Industrial Ethernet Standard. – Tekst: elektronnyj // PROFIBUS. PROFINET: [sajt]. – URL: https://www.profibus.com/technology/profinet (data obrashcheniya: 28.09.2021).
6. Kiberbezopasnost' v sfere geologorazvedki i dobychi nefti i gaza. – Tekst: elektronnyj // Deloitte: [sajt]. – URL: https://www2.deloitte.com/ru/ru/pages/energy-and-resources/articles/tracking-the-trends-2020/2017/cybersecurity-for-upstream-oil-and-gas.html (data obrashcheniya: 04.10.2021).
7. X-Force Threat Intelligence Research Hub. – Tekst: elektronnyj // IBM: [sajt]. – URL: https://www.ibm.com/security/xforce/research-hub (data obrashcheniya: 07.10.2021).
8. VPN-resheniya dlya korporativnyh setej. – Tekst: elektronnyj // TADVISER: [sajt]. – URL: https://www.tadviser.ru/index.php/Stat'ya:VPN-resheniya_dlya_korporativnyh_setej (data obrashcheniya: 17.11.2021).
9. Ellen, Neveux Why Privileged Access Management (PAM) Isn't the Ideal Solution for Managing Vendors / Neveux Ellen. – Tekst: elektronnyj // SecureLink: Third-Party Security: [sajt]. – URL: https://www.securelink.com/blog/why-privileged-access-management-pam-is-not-the-ideal-solution-for-managing-vendors/ (data obrashcheniya: 09.10.2021).
10. Total Cost of Ownership in Technology: Implementation. – Tekst: elektronnyj // TechnologyAdvise: [sajt]. – URL: https://technologyadvice.com/blog/sales/total-cost-ownership-crm-marketing-automation/ (data obrashcheniya: 02.11.2021).